



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

HOW CRITICAL IS CRITICAL INFRASTRUCTURE?

by

David A. Riedman

September 2015

Thesis Advisor:
Second Reader:

Christopher Bellavita
Lauren Wollman

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE September 2015	3. REPORT TYPE AND DATES COVERED Master's thesis		
4. TITLE AND SUBTITLE HOW CRITICAL IS CRITICAL INFRASTRUCTURE?			5. FUNDING NUMBERS	
6. AUTHOR(S) Riedman, David A.				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			12b. DISTRIBUTION CODE A	
13. ABSTRACT (maximum 200 words) The Department of Homeland Security (DHS) holds the statutory mission to protect the nation's critical infrastructure, which is the systems and assets that are nationally significant, and whose losses would result in debilitating consequences to the safety and security of the United States. Based on a meta-analysis of government policies, the current critical infrastructure protection (IP) efforts may be misdirected even though it is the cornerstone mission of the department to prevent terrorism and enhance security. It is likely that the facilities DHS works to protect from terrorism are not the most likely targets for attacks. The manner in which facilities are designated as critical infrastructure may have stemmed from shared experience of many in senior leadership as military strategists rather than from identifying the targets of extremists. Even when a facility is destroyed, the consequences may be more complex than the mission of protecting a single facility against all threats and hazards. These findings can justify reducing the scope of the current IP mission and refining the focus through a risk-based methodology for evaluating only the infrastructure that would cause debilitating impacts on the safety and security of the nation.				
14. SUBJECT TERMS homeland security, critical infrastructure, world trade center, military theory, terrorism			15. NUMBER OF PAGES 155	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

HOW CRITICAL IS CRITICAL INFRASTRUCTURE?

David A. Riedman
Captain, Laytonsville District Volunteer Fire Department, Montgomery County, MD
B.A., Georgetown University, 2008

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
September 2015**

Approved by: Dr. Christopher Bellavita
Thesis Advisor

Dr. Lauren Wollman
Second Reader

Dr. Mohammed Hafez
Chair, Department of National Security Studies

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Department of Homeland Security (DHS) holds the statutory mission to protect the nation's critical infrastructure, which is the systems and assets that are nationally significant, and whose losses would result in debilitating consequences to the safety and security of the United States. Based on a meta-analysis of government policies, the current critical infrastructure protection (IP) efforts may be misdirected even though it is the cornerstone mission of the department to prevent terrorism and enhance security. It is likely that the facilities DHS works to protect from terrorism are not the most likely targets for attacks. The manner in which facilities are designated as critical infrastructure may have stemmed from shared experience of many in senior leadership as military strategists rather than from identifying the targets of extremists. Even when a facility is destroyed, the consequences may be more complex than the mission of protecting a single facility against all threats and hazards. These findings can justify reducing the scope of the current IP mission and refining the focus through a risk-based methodology for evaluating only the infrastructure that would cause debilitating impacts on the safety and security of the nation.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	RESEARCH QUESTION	1
B.	SIGNIFICANCE OF RESEARCH	2
C.	SCOPE OF RESEARCH	2
D.	OVERVIEW OF CHAPTERS.....	4
II.	BACKGROUND AND LITERATURE REVIEW	7
A.	OVERVIEW	7
B.	PRE-9/11 CRITICAL INFRASTRUCTURE IN FEDERAL POLICY	7
C.	9/11–DRIVEN POLICIES AND THE FORMATION OF DHS	8
D.	CURRENT HOMELAND SECURITY POLICIES	11
E.	PEER-REVIEWED WRITING ON CRITICAL INFRASTRUCTURE	14
F.	ANALYSIS OF IMPLICATIONS OF CI DEFINITIONS	15
G.	CRITICAL INFRASTRUCTURE SECTORS	17
H.	COMMERCIAL FACILITIES SECTOR.....	19
I.	CONCLUSION	22
III.	WHAT ARE THE PROBLEMS WITH CURRENT DHS CRITICAL INFRASTRUCTURE POLICIES?	23
A.	NATIONAL ASSET DATABASE.....	23
B.	OVERESTIMATION OF RISK DURING VULNERABILITY ASSESSMENTS OF FACILITIES	26
C.	LOTS OF MONEY AND FEW MEASURABLE RESULTS.....	31
D.	CHANGES TO NATIONAL CRITICAL INFRASTRUCTURE PRIORITIZATION PROGRAM.....	36
E.	EXAMPLE OF THE PROBLEM: CRITICAL INFRASTRUCTURE CHEMICAL SECTOR	40
F.	POTENTIAL SOLUTION—REFINE CRITICAL INFRASTRUCTURE DESIGNATION CRITERIA.....	43
IV.	WHAT IS THE SOURCE OF THE PROBLEM WITH CRITICAL INFRASTRUCTURE PROTECTION POLICY?	45
A.	MILITARY THEORY AND TARGET SELECTION	45
B.	METHODS OF ATTACK	46
1.	Figures and Tables.....	46
2.	Series Warfare.....	47

	3.	Parallel Attack.....	47
	4.	Mass Casualty Attack.....	49
	5.	Mutually Assured Destruction.....	49
C.		WARDEN’S FIVE-RING SYSTEM THEORY.....	50
D.		TERRORISM DIFFERS FROM STRATEGIC WARFARE	53
E.		TERRORISTS HISTORICALLY DO NOT TARGET CRITICAL INFRASTRUCTURE	55
F.		FEAR—THE CRITICAL STRATEGY OF TERRORISM.....	56
G.		OSAMA BIN LADEN’S STRATEGY—OCCUPIED COUNTRY STRATEGY	57
H.		HOMELAND SECURITY ENTERPRISE VERSUS HOMEGROWN VIOLENT EXTREMISTS	58
I.		TERRORIST’S TARGET SELECTION—MAXIMUM EXPOSURE NOT CRITICAL FUNCTIONS.....	58
J.		TERRORIST’S MOTIVATION—ATTENTION AND REWARD	62
K.		DIFFERENCE BETWEEN CRITICAL AND TARGETABLE FACILITIES	63
L.		TARGETABLE LOCATIONS AND EVENTS	68
M.		IMPLICATIONS FOR CRITICAL INFRASTRUCTURE PROTECTION MISSION	68
V.		DESTRUCTION OF FACILITIES DHS CURRENTLY DEFINES AS CRITICAL INFRASTRUCTURE AND THE UNEXPECTED RESULTS	71
A.		CASE STUDY: HOW THE LOSS OF WORLD TRADE CENTER WAS CRITICAL TO REDEVELOPING LOWER MANHATTAN.....	72
	1.	Commercial Real Estate in Manhattan.....	74
	2.	Loss of the World Trade Center.....	76
	3.	Creating New Markets	77
	4.	Cost of 9/11 Attack versus Economic Impacts of Redevelopment	80
	5.	Conclusion	82
	6.	Impact to Critical Infrastructure Definition	83
B.		CASE STUDY: LAS VEGAS CASINOS AND CRITICAL INFRASTRUCTURE	85
	1.	What Gaming Facilities Subsector Members Expect from DHS	87
	2.	Las Vegas Casinos.....	88
	3.	Resiliency within the Las Vegas Casino Industry	91

4.	Individual Gaming Facilities Are Not Critical Infrastructure.....	93
C.	CASE STUDY: SCARCITY OF FUNCTION AND A SINGLE POINT OF FAILURE FOR CHARLESTON, WV WATER SUPPLY	93
VI.	POTENTIAL SOLUTIONS.....	99
A.	RECOMMENDATION: FOLLOW BEST PRACTICES FROM ANALYSIS OF THE UNITED KINGDOM’S CRITICAL INFRASTRUCTURE POLICY.....	100
B.	HOW THE UNITED KINGDOM IS PROTECTING INFRASTRUCTURE	101
C.	RECOMMENDATIONS FOR POLICY REVISION	105
VII.	FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS	109
A.	FINDINGS	109
B.	CONCLUSIONS	111
C.	RECOMMENDATIONS.....	112
D.	OPPORTUNITY FOR FURTHER RESEARCH.....	114
	LIST OF REFERENCES	117
	INITIAL DISTRIBUTION LIST	129

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1.	National Asset Database Growth 2003–2006	24
Figure 2.	National Asset Database Totals by Sector	25
Figure 3.	GAO Comparison of Selected Areas Included in the Department of Homeland Security Vulnerability Assessment Tools and Methods	27
Figure 4.	Length of Department of Homeland Security Vulnerability Assessment Tolls and Methods (Number of Pages and Questions), by Type	30
Figure 5.	Funding for the Infrastructure Protection and Information Security Program (in millions of dollars).....	33
Figure 6.	DHS’s Response to the Mandate in Each of the Five Areas Outlined in the Senate Committee Report	35
Figure 7.	NCIPP Consequence-Based Criteria and Relative Threshold Levels.....	37
Figure 8.	Description and Illustration of an Asset, a Node, a Cluster, and a System.....	39
Figure 9.	Number and Percentage of Facilities Assigned a Final Tier as of January 2013	40
Figure 10.	DHS Chemical Facilities Anti-Terrorism Standards Risk-based Performance Standards	42
Figure 11.	Process of Actions during Strategic Warfare.....	48
Figure 12.	Process of Actions Occurring during Conventional Terrorist Attacks	49
Figure 13.	Warden’s Five-Ring System Theory	51
Figure 14.	Warden’s Five-Ring System Theory Applied to DHS Critical Infrastructure Sectors	54
Figure 15.	Fatalities from Terrorist Attacks	60
Figure 16.	Injuries from Terrorist Attacks	61
Figure 17.	Terrorist Attack Targets by Type.....	62
Figure 18.	Explosive Attacks by Target Type in 62,921 Incidents	64
Figure 19.	Domestic Attacks Causing 1–10 Fatalities/Injuries	65
Figure 20.	New York City Skyline in 1995 and 2014.....	74
Figure 21.	Assessed Property Values in Lower Manhattan between New York City Fiscal Year 1991–2000	75
Figure 22.	Lower Manhattan Commercial Leasing Activity 2001–2014	77

Figure 23.	Measuring the Effects of the September 11, 2001 Attack on New York City	81
Figure 24.	Economic Impact of Redeveloping the World Trade Center Site	81
Figure 25.	Number of Hotel Rooms in Lower Manhattan	83
Figure 26.	Advertising Materials for the new 1 World Trade Center Building	84
Figure 27.	1 World Trade Center website	85
Figure 28.	Image of the “Fabled” Riviera Casino That Closed on May 4, 2015	87
Figure 29.	Population of Las Vegas, NV, by Year.....	89
Figure 30.	Nevada Real Per Capita Income per Year	89
Figure 31.	Monthly Rental Rates in Las Vegas by Year.....	90
Figure 32.	Annual Tax Revenue of Las Vegas Strip Casinos 2001–2012 via University of Las Vegas Center for Gaming Research.....	92
Figure 33.	Las Vegas Visitor Statistics from Visitor and Convention Authority	92
Figure 34.	Interdependencies with Water Sector Infrastructure from National Infrastructure Protection Plan	96
Figure 35.	Using a Risk-Based Approach to Prioritize Sector Resilience Planning	101
Figure 36.	Risks of Terrorist and Other Malicious Attacks	103

LIST OF TABLES

Table 1.	Analysis of Definitions of Critical Infrastructure	16
Table 2.	Terrorist Attacks Causing More than 101 Deaths or Injuries in the United States	66
Table 3.	Original World Trade Center Maximum Leasing Revenue Estimate	78
Table 4.	New World Trade Center Maximum Leasing Revenue Estimate	80
Table 5.	Comparison of U.S. and U.K. Infrastructure Sectors	104

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

9/11	September 11, 2001
BOMA	Building Owners and Managers Association International
CF	commercial facilities
CFATS	Chemical Facilities Anti-Terrorism Standards
CI	critical infrastructure
CI/KR	critical infrastructure and key resources
CNI	critical national infrastructure
DHS	Department of Homeland Security
DOD	Department of Defense
GAO	Government Accountability Office
HSPD	Homeland Security Presidential Directive
IP	infrastructure protection
IRA	Irish Republic Army
LEED	Leadership in Energy and Environmental Design
MAD	Mutually Assured Destruction
MBA	Masters of Business Administration
NADB	National Asset Database
NCIPP	National Critical Infrastructure Prioritization Program
NIPP	National Infrastructure Protection Plan
OIG	Office of Inspector General
PCII	Protected Critical Infrastructure Information
PPD	Presidential Policy Directive
QHSR	Quadrennial Homeland Security Review
UK	United Kingdom
U.S.	United States
UASI	Urban Areas Security Initiative

VSAT	Vulnerability Self-Assessment Tool
WTC	World Trade Center

EXECUTIVE SUMMARY

A. ORIGIN OF THE RESEARCH QUESTION

The owner of a commercial office building can contact the Department of Homeland Security (DHS) and request that a federal representative tour the building to identify vulnerabilities from terrorism. Information about the physical attributes of the facility is entered into a computer program to model risks along with high definition photographs of the exterior. To mitigate the risks from terrorist threats, DHS suggests strategies, such as adding fences, installing electronic access control devices, mounting additional closed circuit television cameras, or conducting random security screenings of visitors. DHS will also provide free training courses for the building's security officers to learn about searching for improvised explosives, handling bomb threats, or identifying terrorists who are conducting surveillance.¹ These services that DHS offers to privately owned commercial facilities (CF) fall under the department's statutory critical infrastructure (CI) protection mission and extend to 77,069 locations designated as "critical infrastructure" in the United States.² How does the recommendation that an office building surround itself with a higher fence align with the federal mission to protect "the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof?"³ Are the federal resources being expended to provide security consultation to

¹ "Protective Security Advisors," June 23, 2015, <http://www.dhs.gov/protective-security-advisors>.

² Office of Inspector General, *Progress in Developing the National Asset Database* (OIG-06-40) (Washington, DC: Department of Homeland Security, 2006), http://www.oig.dhs.gov/assets/Mgmt/OIG_06-40_Jun06.pdf.

³ "What is Critical Infrastructure?" August 26, 2015, <http://www.dhs.gov/what-critical-infrastructure>. Department of Homeland Security.

individual infrastructure facilities helping to accomplish the DHS's cornerstone⁴ mission of protecting the country from terrorist attacks?⁵

B. INTRODUCTION

The chapters of this thesis explore the ideas that not everything designated as critical meets the definition of criticality; the methodologies for evaluating infrastructure are not aligned to the threats from terrorism; when supposedly CI, especially CF, are damaged or destroyed, it turns out the facility was not critical after all; and the overall systems of essential-to-life infrastructure across the country are more resilient than the current methodologies presuppose.

This research is a meta-analysis of government policies on infrastructure protection (IP) to address the question of how these facilities became designated as critical and if the scope of the current IP effort is inhibiting the department's ability to accomplish the mission. This research is limited to the risk evaluation, vulnerability assessment, and protection of physical infrastructure facilities. Rather than simply restating problems with IP that have already been published by the Government Accountability Office (GAO) and Congressional Research Service, this thesis intends to determine the origins of current CI protection policies and the underlying challenges in accomplishing the mission.

C. LITERATURE REVIEW

This research examines the federal IP policies that have been issued over the past 35 years to determine the origin and evolution of the mission. Within these documents, a consensus can be drawn that the definition of the term "critical infrastructure" is the systems and assets that are nationally significant and the loss of which would result in debilitating consequences to the safety and security of the United States. The 10

⁴ Department of Homeland Security, *The 2014 Quadrennial Homeland Security Review* (Washington, DC: Department of Homeland Security, 2014), 6, <http://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf>.

⁵ Ibid.

overarching CI policies⁶ released over the past 19 years consistently describe CI as being nationally significant, providing vital services, being part of an interconnected system, causing debilitating impacts if destroyed, and providing a service necessary to the health and safety of the general public.

Based on the analysis within this thesis, infrastructure that lacks national significance, criticality, and interconnectedness to other infrastructure systems does not meet this definition. The protection strategies for CF presented in the 2010 *NIPP Sector Specific Plan (SSP)—Commercial Facilities* lack information about the continuation of essential-to-life services or protection of nationally significant facilities, which underpins the definitions of CI. As a result, the CF sector serves as an example of the misalignment between what is critical to the nation and what is currently designated as critical by DHS. The CF plan puts emphasis on resilience, openness, and profitability, which does not suggest that critical functions are being carried out or the loss of those functions would result in debilitating impacts to the nation.⁷ While resilience, openness, and profitability are positive business practices, it is ineffective for DHS to be writing plans about concepts that do not correspond to criticality, which is the underlying principle of the IP mission.

This inefficiency creates a discrepancy between the federal policies that define CI and how DHS currently addresses its statutory IP mission to identify, prioritize, and protect the nation's most vital infrastructure.⁸

⁶ *Quadrennial Homeland Security Review, NIPP, PPD-21*, Exec. Order No. 13636, *NIPP, National Security Strategy, HSPD-7, USA PATRIOT Act, PDD/NSC-63*, and Exec. Order No. 13010.

⁷ Department of Homeland Security, *Commercial Facilities Sector-Specific Plan an Annex to the National Infrastructure Protection Plan 2010* (Washington, DC: Department of Homeland Security, 2010), <http://www.dhs.gov/xlibrary/assets/nipp-ssp-commercial-facilities-2010.pdf>.

⁸ The White House, *Presidential Policy Directive—Critical Infrastructure Security and Resilience Presidential Policy Directive/PPD-21—Critical Infrastructure Security and Resilience* (Washington, DC: The White House, 2013), <http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

D. PROBLEMS WITH CURRENT DHS CRITICAL INFRASTRUCTURE POLICIES

This research summarizes the concrete shortfalls with IP that have been documented by other sources including the GAO. A problem with the current policies is that many of the 77,069 facilities do not meet the consensus definition identified in the literature review but are still considered to be “critical infrastructure.” The origin of this issue may have stemmed from the early directive for the newly formed DHS to develop a list of all of the critical facilities across the country.⁹ This thesis explores the challenges from the creation of the National Asset Database (NADB) and the mandate to develop a centralized list of facilities. The problems with the creation of the list were likely compounded by the need to rely on individual facilities to self-assess, and subsequently, overestimate risk. Within this research, the DHS CI chemical sector serves as an example of the challenges that occur with identifying and assessing critical facilities despite spending hundreds of millions of dollars and still resulting in an undetermined reduction in the risk from terrorism.

E. SOURCES OF THE PROBLEM

This research also examines theoretical explanations for the challenges with accomplishing the current CI protection mission. Modern military theories provide a potential explanation for the focus of DHS’s efforts because the threats from terrorism have likely been evaluated based on the education and experience of senior officials with principles of strategic warfare.

Nationally significant infrastructure facilities that can cripple the essential functions of the entire country would be attractive targets for an enemy nation-state to strike with ballistic missile and airpower capabilities during a war. The current terrorist threat comes from homegrown violent extremist and members of terrorist groups who are

⁹ United States Congress, *Committee Reports 109th Congress (2005–2006) House Report 109-713—Part 1* (Washington, DC: United States Congress, 2007), http://thomas.loc.gov/cgi-bin/cpquery/?&sid=cp109alJsu&r_n=hr713p1.109&dbname=cp109&&sel=TOC_192496&.

motivated to inflict mass casualties in the locations most visible and easily accessible.¹⁰ An individual terrorist or a small group of terrorists most likely lack the intelligence, organizational coordination, manpower, and resources to conduct a strategic warfare campaign against nationally significant infrastructure targets with the intent of crippling essential-to-life systems across the country. The strategic warfare approach of developing a static list of vulnerable assets does not match the unpredictable and dynamic threat from terrorism. The current IP policies identify the likely targets of a nation-state army and assume them to be the same targets that terrorists would have the intention and capability of attacking.

F. CASE STUDIES OF THE DESTRUCTION OF CRITICAL FACILITIES

The concept of protecting CI could altogether be a wasted effort because when supposedly CI is destroyed, the impacts are often negligible, or in some cases, even results in economic gains. It should be noted that the loss of human lives can occur with the destruction of critical facilities but the IP mission is not always focused on reducing human losses. In 2013, 32,719 traffic collision fatalities occurred on roadways¹¹ that fall under the CI transportation systems sector but it is the mission of DHS to protect the physical transportation infrastructure from terrorist attacks rather than investing resources to prevent thousands of annual deaths from occurring during vehicle accidents on the highways.¹² It is within the scope of the DHS mission to assess how a bridge could be attacked with explosives by terrorists but not to assess if installing higher guardrails could prevent a car from accidentally driving off the bridge.

Even when terrorists do successfully strike, the consequences may be more complex than making a blanket assumption that all CI facilities should be protected under all circumstances. Case studies of the World Trade Center (WTC) and the Las Vegas

¹⁰ “Countering Violent Extremism,” July 20, 2015, <http://www.dhs.gov/topic/countering-violent-extremism>.

¹¹ National Highway Transportation Safety Administration, *Traffic Safety Facts 2013 Data* (Washington, DC: U.S. Department of Transportation, 2015), <http://www-nrd.nhtsa.dot.gov/Pubs/812181.pdf>.

¹² “Transportation Systems Sector,” March 25, 2013, <http://www.dhs.gov/transportation-systems-sector>.

Strip casinos challenge the general assertion that negative economic consequences always result from the destruction of a “critical” facility. A case study of the 2014 toxic chemical spill into the primary water source serving Charleston, WV provides an example that is contrary to the assumption that the loss of a facility serving as a sole provider of an essential-to-life service results in cascading, debilitating impacts across all infrastructure sectors. The destruction of supposedly critical facilities has demonstrated that greater resilience does occur across infrastructure systems than DHS generally assumes. Instead of focusing protection efforts on potential losses, greater value may be found in understanding existing resiliency.

While it was unforeseeable at the time, the Lower Manhattan area that was most heavily impacted by the September 11, 2001 (9/11) attacks is more valuable today and better positioned for the future than it was prior to 2001. If terrorists cannot cripple this nation by toppling 100-story commercial high-rise buildings, what kinds of facilities would have a debilitating impact on the entire nation if they were destroyed? Instead of being designated “critical,” the majority of infrastructure facilities are insignificant to the functions of the overall system because the loss of these facilities does not cause widespread disruptions to the nation, region, or even the local area. The worst circumstances may spur the greatest opportunity for positive change, which could shift homeland security strategies to focus primarily on effective recovery rather than protecting existing systems.

G. AN ALTERNATIVE STRATEGY

A solution for accomplishing the task of effectively identifying, prioritizing, and protecting CI is refining the criteria for how facilities are determined to be critical. A lower number of critical facilities will reduce the overall scope of the protection mission. To identify facilities more effectively that are CI, DHS should consider using a risk-based approach within a more narrow definition of the term that can be modeled after best practices from the United Kingdom (UK). The United Kingdom uses the designation of “national infrastructure” to emphasize the scope of the mission, which is focused exclusively on the systems that the entire country is dependent on for daily life. For an

infrastructure asset to be considered a national priority, both a high level of criticality and a high likelihood of something negative occurring must exist. Adopting a risk-based approach for both the prioritization of facilities through the likelihood of destruction and evaluation of national impacts can assist DHS in more effectively designating facilities as “critical.”

H. FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

The evidence presented within this thesis argues that DHS is not fulfilling the mission of protecting the infrastructure that is critical to the nation by expending resources on misaligned efforts at thousands of insignificant facilities. These problems are rooted in the current scope of the infrastructure mission being too large but is further complicated because the types of facilities designated as critical may not be the likely targets of terrorists. The few facilities that are critical to the nation are most likely too large, too remote, or too secure for a terrorist group to destroy, or to have an interest in targeting.

On a local and regional level, redundancy and resiliency occur across infrastructure systems allowing affected areas to absorb outages and unaffected areas to provide alternative services. As a backstop, national emergency response capabilities can quickly deliver essential services during outages, such as the bottled water supplied to Charleston, WV following the chemical spill into the water supply. Also, enormous complexity within infrastructure systems makes predicting the impacts of outages extremely difficult, as demonstrated by the unanticipated economic gains in Lower Manhattan following the 9/11 attacks.

Based on this thesis, DHS should ensure that everything designated as “critical” meets the definition of criticality, that the methodologies used for evaluating infrastructure align to the mission of protecting the nation for terrorism, and that protection efforts account for the existing resiliency within the systems that provide essential-to-life infrastructure across the country.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Terrorist attacks can shake the foundations of our biggest buildings, but they cannot touch the foundation of America. These acts shattered steel, but they cannot dent the steel of American resolve.

— President George W. Bush, September 11, 2001¹

The literal foundations of the United States are the CI systems that provide essential-to-life services on which the American people are dependent. These CI systems are “so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.”² Even after the Twin Towers fell, America remained capable of functioning, and President Bush said that night, “the functions of our government continue without interruption...our financial institutions remain strong, and the American economy will be open for business, as well.”³

The terrorist attack had shattered steel but was unable to dent an enormously complex and resilient national system of infrastructure facilities. If terrorists cannot cripple this nation (even on the local level) by toppling 100-story commercial high-rise buildings, what kinds of facilities would have a debilitating impact on the entire nation if they were destroyed?

A. RESEARCH QUESTION

This thesis explores the questions of what infrastructure is critical to the nation and if current IP efforts are aligned to protecting the most critical facilities. The research also addresses the questions of if terrorists are likely to target CI facilities and if the overall concept of protecting infrastructure is actually an unnecessary effort.

¹ “Statement by President George W. Bush in His Address to the Nation,” September 11, 2001, <http://www.911memorial.org/sites/all/files/Statement>.

² “What is Critical Infrastructure?” August 26, 2015, <http://www.dhs.gov/what-critical-infrastructure>.

³ “Statement by President George W. Bush in His Address to the Nation.”

B. SIGNIFICANCE OF RESEARCH

The chapters of this thesis explore the ideas that not everything designated as critical meets the definition of criticality. The methodologies for evaluating infrastructure are not aligned to evaluating the threats from terrorism. When supposedly CI, especially CF, is damaged or destroyed, it turns out that these facilities were not critical after all. Finally, the overall systems of essential-to-life infrastructure across the country are more resilient than the current methodologies presuppose.

The Department of Homeland Security (DHS) has a statutory mission to protect CI⁴ and the *National Strategy for Homeland Security* states,

devastation of even one sector of our critical infrastructure or key resources would have a debilitating effect on our national security. Ensuring the survivability of our critical infrastructure assets, systems, and networks requires that we continue to accurately model their interdependencies and better understand the potential cascading effects that could impact or impede operations in interconnected infrastructures.⁵

Continuously monitoring and analyzing interdependencies within interconnected infrastructure systems is a difficult task. The analysis within this thesis provides justification for reducing the size of the mission to focus on a smaller number of critical facilities.

C. SCOPE OF RESEARCH

This research is a meta-analysis of government policies on IP to address the question of how these facilities became designated as critical and if the scope of the current IP effort is inhibiting the department's ability to accomplish the mission. This research is limited to the risk evaluation, vulnerability assessment, and protection of physical infrastructure facilities. Rather than simply restating problems with IP that have already been published by the Government Accountability Office (GAO) and

⁴ The White House, *Presidential Policy Directive—Critical Infrastructure Security and Resilience* *Presidential Policy Directive/PPD-21—Critical Infrastructure Security and Resilience* (Washington, DC: The White House, 2013), <http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

⁵ Homeland Security Council, *National Strategy for Homeland Security* (Washington, DC: The White House, 2007), 27, http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf.

Congressional Research Service, this thesis intends to determine the origins of current CI protection policies and the underlying challenges in accomplishing the mission.

Homeland Security Presidential Directive 7 calls for “strategic improvements in security that can make it more difficult for attacks to succeed and can lessen the impact of attacks that may occur. In addition to strategic enhancements, tactical security improvements can be rapidly implemented to deter, mitigate, or neutralize potential attacks.”⁶ *Presidential Policy Directive 21*,⁷ the overarching federal policy that dictates IP, is also focused primarily on the physical protection of facilities from terrorist attacks, which is why this research is focused exclusively on that aspect of the CI protection mission.

This research does not include cyber and all-hazard (hurricanes, earthquakes, and other natural hazards) threats. The nature and source of cyber threats are constantly evolving and with nearly all aspects of infrastructure, business, and personal life connected to the Internet, these threats are too broad and uncertain for the purposes of this research. The GAO has also reported that DHS lacks a strategy for defining, identifying, and assessing the cyber risks to buildings,⁸ thus, this research focuses on the more established physical security mission. All-hazards planning is rooted in the evaluation of the risks from predictable or forecastable natural disasters for determining how mitigation efforts (e.g., building a flood wall or adding structural shoring) can hedge those risks. The unpredictability and uncertainty of intentional terrorist attacks on physical infrastructure facilities requires completely different protective measures and evaluations of risk for determining vulnerability. According to Homeland Security Secretary Jeh Johnson’s May 2015 remarks, “counterterrorism must remain the cornerstone of our Department’s overall homeland security mission. It’s the reason the

⁶ The White House, *Homeland Security Presidential Directive 7* (Washington, DC: The White House, 2003), <http://www.dhs.gov/homeland-security-presidential-directive-7>.

⁷ The White House, *Presidential Policy Directive—Critical Infrastructure Security and Resilience* *Presidential Policy Directive/PPD-21—Critical Infrastructure Security and Resilience*.

⁸ Government Accountability Office, *Federal Facility Cyber Security DHS and GSA Should Address Cyber Risk to Building and Access Control Systems* (GAO-15-6) (Washington, DC: U.S. Government Accountability Office, 2014), <http://www.gao.gov/assets/670/667512.pdf>.

Department was created by Congress in the wake of 9/11.”⁹ Cyber intrusions and natural disasters are not the primary focus of DHS, which is why this research focuses on the protection of physical infrastructure from terrorist attacks.

This research also does not evaluate classified and protected CI information.¹⁰ Infrastructure is public by the nature of the services the facilities provide the consumers (who are the general public) and the private ownership of the majority of facilities. Since protection of this infrastructure is a shared mission between the government and private industry, openly sharing information about what is critical is necessary to coordinate effectively across multiple industries, private owners, local governments, and the public. The GAO has highlighted that the “Department of Homeland Security is not positioned to manage an integrated and coordinated government approach for assessments [of critical infrastructure facilities] as called for in the National Infrastructure Protection Plan.”¹¹ Classification likely contributes to the lack of integration and coordination between all parties involved in IP by preventing the open sharing of information. This thesis investigates openly available information and is not an evaluation of the classified tiered list of infrastructure facilities maintained by the DHS Security Office of Infrastructure Protection.

D. OVERVIEW OF CHAPTERS

This thesis is organized to provide the reader with the background on CI policies, explain the problems with the current CI protection efforts, and offer explanations for the root of these problems. The thesis then explores cases studies that challenge general assumptions about CI facilities and offers an alternative strategy as a solution.

⁹ Jeh Charles Johnson, “Remarks By Secretary Jeh Charles Johnson On “The New Realities Of Homeland Security” As Part of the Landon Lecture Series on Public Issues—As Prepared for Delivery,” Department of Homeland Security, May 27, 2015, <http://www.dhs.gov/news/2015/05/27/remarks-secretary-homeland-security-jeh-charles-johnson-%E2%80%9Cnew-realities-homeland>.

¹⁰ “Protected Critical Infrastructure Information (PCII) Program,” June 18, 2014, <http://www.dhs.gov/protected-critical-infrastructure-information-pcii-program>.

¹¹ Government Accountability Office, *Critical Infrastructure Protection DHS Action Needed to Enhance Integration and Coordination of Vulnerability Assessment Efforts* (GAO-14-507) (Washington, DC: U.S. Government Accountability Office, 2014), <http://www.gao.gov/assets/670/665788.pdf>.

Chapter II, the literature review, examines the federal IP policies that have been issued over the past 35 years to determine the origin and evolution of the mission. Within these documents, a consensus can be drawn that the definition of the term “critical infrastructure” is the systems and assets that are nationally significant and the loss of which would result in debilitating consequences to the safety and security of the United States.

Chapter III, the problems with current DHS CI policies, summarizes the concrete shortfalls with IP that have been documented. An underlying problem is that many of the currently designated CI facilities do not meet the consensus definition identified in the literature review. This chapter also explores the challenges from the mandate to develop a centralized list of facilities and the problems with relying on individual facilities to self-assess, and subsequently, overestimate risk.

Chapter IV, the source of the problems, examines theoretical explanations for the challenges with accomplishing the current CI protection mission. Modern military theories provide a potential explanation for the focus of DHS’s efforts because the threats from terrorism have likely been evaluated based on the education and experience of senior officials with principles of strategic warfare. The strategic warfare approach of developing a static list of vulnerable assets does not match the unpredictable and dynamic threat from terrorism. The current IP policies identify the likely targets of a nation-state army and assume them to be the same targets that terrorists would have the intention and capability of attacking.

Chapter V, case studies of the destruction of critical facilities, explores the concept of protecting CI that could altogether be a wasted effort because when supposedly CI is destroyed, the impacts are often negligible, or in some cases, even results in economic gains.

Chapter VI, an alternative strategy, provides a solution for accomplishing the task of effectively identifying, prioritizing, and protecting CI, and refines the criteria for how facilities are determined to be critical. A lower number of critical facilities will reduce the overall scope of the protection mission. To identify facilities more effectively that are CI,

the DHS should consider using a risk-based approach within a more narrow definition of the term that can be modeled after best practices from the United Kingdom (UK).

II. BACKGROUND AND LITERATURE REVIEW

A. OVERVIEW

Over the past 30 years, federal government policies have stated the importance of protecting CI. Key documents in defining this protection mission have included President Clinton's *Executive Order 13010*, the *USA PATRIOT Act*, *Presidential Policy Directive 63*, multiple iterations of the *National Critical Infrastructure Protection Plan* (NIPP), and the *2014 Quadrennial Homeland Security Review*. As the concepts within the policies develop over time, the definitions of CI continues to remain focused on the systems and assets that are nationally significant and their losses result in debilitating consequences to the safety and security of the United States.

B. PRE-9/11 CRITICAL INFRASTRUCTURE IN FEDERAL POLICY

Prior to the establishment of DHS, the concept of CI existed in federal policies. In the 1980s, the Congressional Budget Office determined CI to be systems that "share common characteristics of capital intensiveness and high public investment at all levels of government." Infrastructure was divided into seven critical sectors: "highways, public transit, wastewater treatment, water resources, air traffic control, airports, and municipal water supply."¹² While this list did not include other sectors that are now considered critical, such as communications systems, the methodology of the analysis used during the time period was based on the assumption stated in the 1988 Congressional report that CI "excludes some facilities often thought of as infrastructure where the initial onus of responsibility is on private individuals."¹³

Prior to September 11, 2001 (9/11), President Clinton's Executive Order 13010 defined CI as being "so vital that their incapacity or destruction would have a debilitating

¹² U.S. Congressional Budget Office, *Public Works Infrastructure: Policy Considerations for the 1980s* (Washington, DC: U.S. Government Printing Office, 1983), 1.

¹³ U.S. Congressional Budget Office, *New Directions for the Nation's Public Works* (Washington, DC: U.S. Government Printing Office, 1988), xi-xii.

impact on the defense or economic security of the United States.”¹⁴ PDD/NSC-63 follows the same rhetoric by stating that CI is “so vital to the Nation that their incapacity or destruction would have a debilitating impact on national security, national economic security, and/or national public health and safety.”¹⁵ The protection mission of the directive focused on identifying the “minimum essential infrastructure in each sector,” which would include only the infrastructure that would “significantly damage the United States” if it was attacked.¹⁶ In response to the requirements of PDD/NSC-63 for government components to provide their own specific IP plans, the Department of Defense (DOD) articulated some of the challenges to meeting the directive’s requirements. The 1998 *DOD Critical Infrastructure Protection Plan* asserts that “the complexity of the problem manifests itself in the lack of shared understanding of the terminology and the variety of different perceptions held by the Department’s and the nation’s leadership about the meaning and discipline of designing evolving, assuring, and protecting infrastructure.”¹⁷ To address PDD-63’s requirement to determine the minimum essential infrastructure in each sector, the DOD plan states, “this begs the questions: essential or critical to whom or for what?,”¹⁸ which shows the continued challenges in determining what constitutes infrastructure as critical.

C. 9/11–DRIVEN POLICIES AND THE FORMATION OF DHS

In the Bush Administration’s original proposal for defining the roles of DHS in 2002, identifying and protecting CI were specific tasks for the department. While the

¹⁴ Exec. Order No. 13010, Critical Infrastructure Protection (1996), accessed July 26, 2015, <http://fas.org/irp/offdocs/eo13010.htm>.

¹⁵ The White House, *Presidential Decision Directive/NSC-63* (Washington, DC: The White House, 1998), <http://www.fas.org/irp/offdocs/pdd/pdd-63.htm>.

¹⁶ Ibid.

¹⁷ Department of Defense, *The Department of Defense Critical Infrastructure Protection Plan Version 1.0* (Washington, DC: Department of Defense, 1998), <http://www.fas.org/irp/offdocs/pdd/DOD-CIP-Plan.htm>.

¹⁸ Ibid.

proposal stated the mission, the definition of CI was lacking, which made the success in meeting the IP mission difficult to measure.¹⁹

While infrastructure systems have been determined to be critical through a variety of measures, the USA PATRIOT Act provides a concrete definition that is cited within subsequent policies, national plans, and directives pertaining to CI. The USA PATRIOT Act states that CI is “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such system and assets would have debilitating impact on security, national economic security, and national public health or safety, or any combination of those matters.”²⁰

In 2003, Homeland Security Presidential Directive (HSPD): Critical Infrastructure Identification, Prioritization, and Protect, gave the Secretary of Homeland Security the statutory responsibility of “coordinating the overall national effort to enhance the protection of the CI and key resources of the United States.”²¹ The CI protection mission was rooted in protecting infrastructure that would cause a catastrophic loss of life, impair the government’s ability to function, or cripple the economy.²² This directive also assigned the Secretary of Homeland Security with the responsibility for designating events as “national special security events” but that assignment within this directive is not stated to be directly related to the IP missions.²³

Prior to the most current version of the NIPP, the first *Interim National Infrastructure Protection Plan* published in February 2005, offered the definition of then critical infrastructure and key resources (CI/KR) as the “infrastructure and key resources

¹⁹ John Moteff, Claudia Copeland, and John Fischer, *Critical Infrastructures: What Makes an Infrastructure Critical?* (CRS Report No. RL31556) (Washington, DC: Congressional Research Service, 2003), <http://fas.org/irp/crs/RL31556.pdf>.

²⁰ 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. §5195c(e) (2001)).

²¹ The White House, *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection* (Washington, DC: The White House, 2003), Section 11, <http://www.dhs.gov/homeland-security-presidential-directive-7>.

²² *Ibid.*, Section 7.

²³ *Ibid.*, Section 26.

vital to our national security, economic vitality, and way of life.”²⁴ An attack on the nation’s key resources would have “cascading effects” and cause “large-scale human casualties and property destruction...also profound damage to the national prestige, morale, and confidence.”²⁵ The plan proposed that a two-pronged approach of reducing vulnerabilities and taking threat-initiated actions as the best strategy for reducing risks to infrastructure.²⁶ Being the first iteration of the NIPP, the plan focuses on data collection (through the national CI/KR inventory) and the identification of risks rather than the concept of resilient systems, which appear in the newer versions of the document. The interim NIPP was formalized in the *2009 National Infrastructure Protection Plan—Partnering to Enhance Protection and Resiliency*. A significant change in the 2009 version was the increased focus on the concept of resiliency and a three-pronged approach of deterring threats, mitigating vulnerabilities, and minimizing consequences (resiliency).²⁷

The *Guide to Critical Infrastructure and Key Resources Protection at the State, Regional, Local, Tribal, and Territorial Level* published in September 2008 defines CI as “the assets, systems, and network that, if damaged, would result in significant consequences—where the degree of impact on economic security, public health and safety, public confidence, loss of life, or some combination of these adverse outcomes has been established through the criteria identified.”²⁸ In describing the methodology for gathering information about CI, the document explains, “some sectors include certain classes of assets, systems, or networks that are unlikely to be the target of an attack and/or are relatively inconsequential if attacked. These assets will not need to be

²⁴ Department of Homeland Security, *Interim National Infrastructure Protection Plan* (Washington, DC: Department of Homeland Security, 2005), 1, <https://net.educause.edu/ir/library/pdf/csd3754.pdf>.

²⁵ Ibid.

²⁶ Ibid., 10.

²⁷ Department of Homeland Security, *National Infrastructure Protection Plan—Partnering to Enhance Protection and Resiliency* (Washington, DC: Department of Homeland Security, 2009), 7, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

²⁸ Department of Homeland Security, *A Guide to Critical Infrastructure and Key Resources Protection at the State, Regional, Local, Tribal, and Territorial Level* (Washington, DC: Department of Homeland Security, 2008), 31, http://www.dhs.gov/xlibrary/assets/nipp_srltt_guide.pdf.

identified.”²⁹ It is an important assertion that all infrastructure systems are not critical and should not be identified because not all infrastructure facilities are significant.

The *National Critical Infrastructure Prioritization Program* (NIPP) called for developing a list of the nation’s “highest priority infrastructure” based on “effects of an event on public health and safety, and economic, psychological, and government mission impacts.”³⁰ This analysis was consequence-based around five levels of impact. Following the CI definitions from other federal documents, Level-1 and Level-2 infrastructure losses would have “nationally or multi-state significant loss of life, public health, economic, and/or national security impacts.”³¹

D. CURRENT HOMELAND SECURITY POLICIES

The *2013 National Infrastructure Protection Plan (NIPP)* suggests that identifying CI comes through “identifying the assets, systems, and networks that are essential to the continued operation, considering associated dependencies and interdependencies. The federal government identifies and prioritizes nationally significant CI base upon statutory definition and national considerations.”³² According to the NIPP, risk should be managed by “understanding the criticality as well as the associated interdependencies of infrastructure. Lifeline functions such as communications, energy, transportation, and water are the most critical infrastructure sectors.”³³

²⁹ Department of Homeland Security, *A Guide to Critical Infrastructure and Key Resources Protection at the State, Regional, Local, Tribal, and Territorial Level*, 33.

³⁰ “About: Infrastructure Information Collection Division,” July 14, 2015, <http://www.dhs.gov/about-infrastructure-information-collection-division>.

³¹ Harris County Office of Homeland Security and Emergency Management, *Lessons Learned Information Sharing, Infrastructure Systems: Developing a Critical Infrastructure and Key Resources (CIKR) Plan* (Houston, TX: Harris County Office of Homeland Security and Emergency Management, 2014), 3, <http://www.readyharris.org/external/content/document/1829/2233754/1/20140825%20LLIS%20ICKR.pdf>.

³² Department of Homeland Security, *National Infrastructure Protection Plan 2013—Partnering for Critical Infrastructure Security and Resilience* (Washington, DC: Department of Homeland Security, 2013), 16, http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf.

³³ *Ibid.*, 17.

Presidential Policy Directive 21—Critical Infrastructure Security and Resilience (PPD-21) released in February 2013 asserts, “the Nation’s critical infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure—including assets, networks, and systems—that are vital to public confidence and the Nation’s safety, prosperity, and well-being.”³⁴ A solution for securing infrastructure is offered through developing resilience, which will allow “critical infrastructure to be secure and able to withstand and rapidly recover from all hazards.” Further, “all Federal department and agency heads are responsible for the identification, prioritization, assessment, remediation, and security of their respective internal CI that supports primary mission essential functions. Such infrastructure shall be addressed in the plans and execution of the requirements in the National Continuity Policy.”³⁵ The policy calls on “the Federal Government to work with CI owners and operators to take proactive steps to manage risk and strengthen the security and resilience of the Nation’s critical infrastructure, considering all hazards that could have a debilitating impact on national security, economic stability, public health, and safety, or any combination thereof.”³⁶ The requirements within PPD-21 emphasize that hazards to CI must have a “debilitating” impact on the nation.³⁷ The document’s glossary defines

the term critical infrastructure, provided in section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c(e)), as namely systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.³⁸

Resilience is a concept interconnected with IP. The *2013 NIPP Supplemental Tool: Incorporating Resilience into Critical Infrastructure Projects* defines resilience as

³⁴ The White House, *Presidential Policy Directive—Critical Infrastructure Security and Resilience* *Presidential Policy Directive/PPD-21—Critical Infrastructure Security and Resilience*.

³⁵ Ibid.

³⁶ Ibid.

³⁷ Ibid.

³⁸ Ibid.

“the ability to prepare for and adapt to changing conditions and withstand and recover from deliberate attacks, accident, or national occurring threats or incidents. Resilient infrastructure systems are flexible and agile and should be able to bounce back after disruption.”³⁹ While the *NIPP Supplemental Tool* offers a list of recommendations for increasing the resilience of a CI sector, recommendations like “conduct vulnerability assessments to identify known and future risks” and “build redundancy into infrastructure systems” are a far stretch from providing actionable recommendations for allowing facilities to “bounce back” following disruptions. The *NIPP Supplemental Tool* restates the factors contributing to CI failures without offering solutions.

Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection frames infrastructure facilities that must be protected as the sites that “threaten national security, cause mass casualties, weaken our economy, and damage public morale and confidence.” The CI facilities provide the “essential services that underpin American society.”⁴⁰

CI is also a topic within the *2014 Quadrennial Homeland Security Review* (QHSR). In the context of natural disasters, the loss of CI causes “widespread disruptions of essential services across the country.”⁴¹ The QHSR states that CI provides “essential services that underpin the American way of life” and “interconnected infrastructure consists of multiple systems that rely on one another to greater degrees for their operation.”⁴² Following the same concepts as the 2013 NIPP, the QHSR suggests infrastructure that is “more reliable, efficient, and resilient”⁴³ and that can be a solution to protecting the delivery of essential services.

³⁹ Department of Homeland Security, *Supplemental Tool: Incorporating Resilience into Critical Infrastructure Projects* (Washington, DC: Department of Homeland Security, 2013), 1, http://www.dhs.gov/sites/default/files/publications/NIPP%202013%20Supplement_Incorporating%20Resilience%20into%20CI%20Projects_508.pdf.

⁴⁰ The White House, *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection*.

⁴¹ Department of Homeland Security, *The 2014 Quadrennial Homeland Security Review* (Washington, DC: Department of Homeland Security, 2014), 22, <http://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf>.

⁴² *Ibid.*, 23.

⁴³ Department of Homeland Security, *The 2014 Quadrennial Homeland Security Review*, 24.

Executive Order 13636—Improving Critical Infrastructure Cybersecurity published in 2013 follows a similar definition as the USA PATRIOT Act by stating that the loss of CI has “a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”⁴⁴ Section 9 specifies that efforts should be focused on the CI systems that cause catastrophic national or regional impacts.

E. PEER-REVIEWED WRITING ON CRITICAL INFRASTRUCTURE

Peer reviewed articles on CI utilize the same general definition that CI is the interconnected systems that can have debilitating impacts to the nation if they fail.

In studying the cascading impacts of infrastructure failure, CI is defined as the

complex systems of components that ensure production, transport, communication, health, safety, and any other activities necessary for a society’s (country’s) needs. Its disruption or destruction would affect the teams working at these complexes, the surrounding structures, public health and safety, the economy, and national security.⁴⁵

Interdependency between CI systems is used as a basic assumption for in-depth analysis of systems. A risk analysis approach to studying CI focused on the “rippling effect of hazardous disturbances (such as natural or willful hazards) to any CI can be far-reaching and long-lasting. This forms a cascading effect, which may be far greater than the initial loss inflicted by the direct disturbance.”⁴⁶

An analysis of engineering resilience into physical facilities defined CI as “significant pieces of plant and equipment, such as power stations and motorways. High population densities in cities, and the increasing interconnectedness of the services and

⁴⁴ Exec. Order No. 13636—Improving Critical Infrastructure Cybersecurity (2013), 3, <http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf>.

⁴⁵ Farid Kadri, Bibiga Birregah, and Eric Châtelet, “The Impact of Natural Disasters on Critical Infrastructures: A Domino Effect-based Study,” *Journal of Homeland Security and Emergency Management* 11, no. 2 (2014): 217–241, <http://dx.doi.org/10.1515/jhsem-2012-0077>.

⁴⁶ Pu Jiang and Yacov Y. Haimes, “Risk Management for Leontief-based Interdependent Systems,” *Risk Analysis* 24, no. 5 (2004): 1215–1229, <http://dx.doi.org/10.1111/j.0272-4332.2004.00520.x>.

supply chains that sustain them.”⁴⁷ A study of engineering resilient transportation systems proposed that transportation infrastructure that would cause debilitating impacts should be reengineered to be durable to lessen the impact from natural disasters.⁴⁸ A similar analysis of security for physical facilities defined CI as the “infrastructures are so vital that incapacity would have far-reaching and debilitating effects on the United States and her allies.”⁴⁹

Joseph’s article “Critical Business Elements and Key Assets” identifies the additional challenge that federal policy does not provide specific guidelines for determining criticality. “The scope and complexity of CI sectors can make this a daunting task to identify which specific assets are critical. Most of these guidelines do not provide specific basis for determining ‘criticality’ in the broader economic or social welfare impacts as called for in federal critical infrastructure strategies.”⁵⁰

F. ANALYSIS OF IMPLICATIONS OF CI DEFINITIONS

Federal government reports, plans, policies, and directives from the 1980s to today, emphasize that CI is the interconnected systems that can cause debilitating impacts to the safety and security of the nation if they are destroyed by natural disasters or terrorism. Scholarly studies of CI use the same definitions for framing their analysis of the topic.

As demonstrated by Table 1, 13 overarching federal government policies released over the past 19 years consistently describe CI as being nationally significant, providing vital services, being part of an interconnected system, causing debilitating impacts if

⁴⁷ Christopher D. F. Rogers et al., “Resistance and Resilience-Paradigms for Critical Local Infrastructure,” *Proceedings of the Institution of Civil Engineers: Mechanical Engineering* 165, no. 2 (2012): 73–83, <http://search.proquest.com/docview/1223110482?accountid=12702>.

⁴⁸ Institute of Transportation Engineers, “Ahead of the Storm: Engineering for Disaster,” *ITE Journal*, 2013, <http://search.proquest.com/docview/1468925507?accountid=12702>.

⁴⁹ Lee Parrish and Mark Leary, “Secure Global Collaboration among Critical Infrastructures,” *Information Security Journal: A Global Perspective* 18, no. 2 (2009): 57–63, <http://search.proquest.com/docview/743437113?accountid=12702>.

⁵⁰ Anthony Joseph, “Critical Business Elements and Key Assets,” *Security* 43, no. 8 (2006): 40–41, <http://search.proquest.com/docview/197794745?accountid=12702>.

destroyed, and providing a service necessary to the health and safety of the general public.

Table 1. Analysis of Definitions of Critical Infrastructure

Year	Document	Nationally Significant	Provide Vital Service	Interdependent System	Debilitating Impact	Safety of Public
2014	Quadrennial Homeland Security Review	X	X	X	X	X
2013	NIPP	X	X	X		X
2013	PPD-21: CI	X	X	X	X	X
2013	Executive Order 13636	X	X	X	X	X
2011	NCIPP Level 1/Level 2 Program	X	X	X	X	X
2009	NIPP	X	X	X	X	X
2008	NIPP SRTLTT Guide	X	X	X	X	X
2007	National Security Strategy ⁵¹	X	X	X	X	X
2005	Interim NIPP	X	X	X	X	X
2003	HSPD 7	X	X	X	X	X
2001	USA PATRIOT Act	X	X	X	X	X
1998	PDD/NSC-63	X	X	X	X	X
1996	Executive Order 13010	X	X		X	X
1988	Congressional Budget Office Report	X	X			

DHS currently provides a wide-ranging list of facilities within 16 different sectors that are considered to be critical.⁵² The emphasis on national significance, vital services, interdependent systems, debilitating impacts, and safety of the public in each prominent

⁵¹ Homeland Security Council, *National Strategy for Homeland Security*, 27.

⁵² “Critical Infrastructure Sectors,” June 12, 2014, <http://www.dhs.gov/critical-infrastructure-sectors>.

CI definition show a consensus in the definition of the term. An agreed upon definition of what is critical allows for the interpretation of what is not CI.

G. CRITICAL INFRASTRUCTURE SECTORS

Presidential Policy Directive 21: Critical Infrastructure Security and Resilience identifies 16 different sectors⁵³ into which CI facilities are organized. These sectors and various subsectors, components, industries, segments, and disciplines include:

- Chemical Sector
 - Basic Chemical Component
 - Specialty Chemical Component
 - Agricultural Chemical Component
 - Pharmaceuticals Component
 - Consumer Products Component
- Commercial Facilities Sector
 - Public Assembly Subsector
 - Sports Leagues Subsector
 - Gaming Subsector
 - Lodging Subsector
 - Outdoor Events Subsector
 - Entertainment and Media Subsector
 - Real Estate Subsector
 - Retail Subsector
- Communications Sector
- Critical Manufacturing Sector
 - Primary Metal Manufacturing Industry
 - Machinery Manufacturing Industry
 - Electrical Equipment, Appliance, and Component Manufacturing Industry

⁵³ The White House, *Presidential Policy Directive—Critical Infrastructure Security and Resilience* *Presidential Policy Directive/PPD-21—Critical Infrastructure Security and Resilience*.

- Transportation Equipment Manufacturing Industry
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector
 - Law Enforcement Discipline
 - Fire and Emergency Services Discipline
 - Emergency Management Discipline
 - Emergency Medical Services Discipline
 - Public Works Discipline
- Energy Sector
 - Electricity Segment
 - Petroleum Segment
 - Natural Gas Segment
- Food and Agriculture Sector
- Government facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Transportation Sector
 - Aviation Subsector
 - Highway Infrastructure and Motor Carrier Subsector
 - Maritime Transportation System Subsector
 - Mass Transit and Passenger Rail Subsector
 - Pipeline System Subsector
 - Freight Rail Subsector
 - Postal and Shipping Subsector
- Water and Wastewater Systems Sector⁵⁴

⁵⁴ “Critical Infrastructure Sectors.”

H. COMMERCIAL FACILITIES SECTOR

A sector that can serve as an example for how to re-categorize facilities currently designated as critical is the CF sector. The mission of protecting the CF sector presented in the 2010 *NIPP Sector Specific Plan (SSP)—Commercial Facilities* lacks emphasis on “essential-to-life services” referenced in other descriptions of CI. The sector’s mission also lacks emphasis on debilitating economic damage to the nation, and instead, focuses on the operations of individual businesses:

The Commercial Facilities Sector envisions a secure, resilient, and profitable sector in which effective and non-obstructive risk management programs instill a positive sense of safety and security in the public and sustain favorable business environments that are conducive to attracting and retaining employees, tenants, and customers.⁵⁵

The emphasis on resilience, openness, and private sector profitability does not suggest that critical functions are being carried out, and the loss of those functions would result in debilitating impacts to the nation, rather than losses to individual private sector corporations. While CI systems can be mapped to key nodes causing failure across multiple systems, the CF sector supplement section on prioritizing infrastructures states that it does “not believe it is appropriate to develop a single overarching prioritized list of assets for the Commercial Facilities Sector. Instead, assets are categorized using a consequence methodology that allows the Commercial Facilities Sector Specific Agencies to drive sector-wide protection efforts.”⁵⁶ Further showing the lack of interconnected systems within the CF sector, “individual owners and operators apply effective implementation and evaluation of protective programs and resilience strategies.”⁵⁷

The *National Infrastructure Protection Plan—Commercial Facilities Sector Specific Plan* uses dollar figures and statistics to attempt to show the national importance of the CF sectors. Examples, such as “the retail industry generates \$4.6 trillion in annual

⁵⁵ Department of Homeland Security, *Commercial Facilities Sector-Specific Plan an Annex to the National Infrastructure Protection Plan 2010* (Washington, DC: Department of Homeland Security, 2010), <http://www.dhs.gov/xlibrary/assets/nipp-ssp-commercial-facilities-2010.pdf>.

⁵⁶ Ibid., 3.

⁵⁷ Ibid.

sales” and “35 million Americans work in office buildings,”⁵⁸ are attempts to show the national implications of losses to the sector but CF are not a single entity. An attack or multiple attacks on CF would not result in massive losses across the entire sector. The document cites, “1.6 million U.S. retail establishments that employ 24 million Americans.” If simultaneous terrorist attacks destroyed 100 different retail establishments with each business having \$10 million in annual revenue (well above the national average⁵⁹), the losses would be less than .04% of the entire retail industry’s annual total revenue (\$1 billion in losses compared with \$4.6 trillion in annual revenue).

The vulnerability of the facilities in the sector is attributed to the number of people occupying the buildings rather than the importance of the actual structures:

The CF Sector is one of the few CIKR sectors that terrorists have attacked successfully. Commercial facilities are especially vulnerable due to the large inventory of buildings across the Nation that are open to the public and are populated by large numbers of people on a daily basis. Commercial facilities are designed to be welcoming and attractive to customers and can be contrary to design security principals.⁶⁰

The factors used to assess the criticality of CF are not based around performance measures that relate to providing essential-to-life functions or measures impacting national economic security. As a counter example, the energy sector measures ability to deliver power to customers. The CF sector uses attributes, such as the “height of building” and “number of rooms,” as measures of importance but neither of these factors direct measures of criticality of the facility. An electric power plant measures its performance in megawatts of power produced not by the height of the smoke stack, which is just a physical attribute of the facility. Within CF, a higher number of rooms do not mean that the facility is always fully occupied or more critical than a smaller building. The factors listed as the “attributes of interest” for the CF sector are seemingly

⁵⁸ Department of Homeland Security, *Commercial Facilities Sector-Specific Plan an Annex to the National Infrastructure Protection Plan 2010*, 7.

⁵⁹ “Small Business Overview,” 2015, <http://asq.org/learn-about-quality/small-business/overview/overview.html>.

⁶⁰ Department of Homeland Security, *Commercial Facilities Sector-Specific Plan an Annex to the National Infrastructure Protection Plan 2010*, 8.

arbitrary to the function of facility. These arbitrary attributes of interest identified within the CF sector plan include:

- Facility Location: General geographic situation (e.g., financial district, industrial park).
- Facility Proximity: Proximity to high-risk enterprises (e.g., adjacency to an iconic landmark or important federal building).
- Facility Size: Height, footprint, number of floors, hotel rooms, apartments, public areas, and exhibition/retail space.
- Facility Capacity/Attendance: Design population annual attendance (e.g., the number of tenants in an office building, spectators at a sporting event, and visitors/participants at an outdoor event).
- Facility Type: Purpose or use of the facility (e.g., office building, stadium, hotel, amusement park).
- Geographical Area: Defined by local government, it includes prestigious commercial (e.g., retail, hotels, and office buildings) and residential assets that are nationally recognized as a tourist destination and unified economic entity.
- Facility Functions: Types of events held in the facility (e.g., national sporting events, political conventions, and controversial exhibitions).
- Facility Value: Iconic and economic status of the facility (e.g., historical status, owner, tenants, and clientele).⁶¹

Regulatory agencies were developed more than 100 years ago to protect consumers, the government, and the economic stability of the United States from mismanagement of essential services (manufacturing, banking, transportation, etc.).⁶² “The commercial facilities sector is considered a non-regulatory sector” and has “no obligations that require owners to disclose information to the government.”⁶³ While this lack of regulation can seemingly be a barrier to IP, it is also an indication of the lack of criticality within the sector due the historic absence of government interest and oversight.

⁶¹ Department of Homeland Security, *Commercial Facilities Sector-Specific Plan an Annex to the National Infrastructure Protection Plan 2010*, 20.

⁶² “A Brief History of Administrative Government,” 2015, <http://www.foreffectivegov.org/node/3461>.

⁶³ Department of Homeland Security, *Commercial Facilities Sector-Specific Plan an Annex to the National Infrastructure Protection Plan 2010*, 30.

I. CONCLUSION

Federal government documents over the past 35 years have a consensus in their definition of CI being the systems and assets that are nationally significant and the facility losses result in debilitating consequences to the safety and security of the United States. Based on this analysis of the literature, infrastructure that lacks national significance, criticality, and interconnectedness of other infrastructure systems does not meet the definition of “critical infrastructure.” It represents a discrepancy between the federal policies that define CI and how DHS currently views infrastructure facilities. While DHS takes an all-inclusive approach to include as many facilities as possible under the designation as “critical,” CI has consistently been defined as only the systems that are nationally significant. This problem is apparent when looking at the CF sector due to the measures of criticality that relate to physical attributes of the facilities and do not relate to nationally significant essential-to-life services or maintaining economic security.

To challenge the current CI protection policies relating to CF further, case studies of the World Trade Center (WTC) and the Las Vegas Strip challenge general assertions of the negative economic impact occurring after the destruction of a “critical” commercial facility. A case study of the 2014 toxic chemical spill into the primary water source serving Charleston, WV also provides an example that is contrary to the concept that the loss of a facility serving as sole provider of an essential-to-life service results in debilitating impacts across all infrastructure sectors within a local area.

III. WHAT ARE THE PROBLEMS WITH CURRENT DHS CRITICAL INFRASTRUCTURE POLICIES?

As demonstrated in the literature review, numerous federal government documents come to a consensus in their definition of CI as a facility that serves as a single or substantial provider of an essential function or service interconnected to other infrastructure systems. The problem with DHS policies is that many facilities do not meet this definition but are still considered to be “critical infrastructure.” The origin of this issue may stem from the directive for DHS to develop a list of all the critical facilities around the country. Creating a national list of assets across 16 sectors of infrastructure resulted in a generally inclusive approach to identifying facilities.

A. NATIONAL ASSET DATABASE

Subtitle A of title II of the Homeland Security Act of 2002 created the NADB to categorize and prioritize CI facilities across the country. The first DHS Infrastructure Protection Risk Management Division list identified 160 nationally critical sites.⁶⁴

The 2007 Department of Homeland Security Authorization Act Sec. 704 directs the Secretary of Homeland Security⁶⁵ to:

(A) Maintaining a catalog of the Nation’s most at risk infrastructure in a single repository of national assets known as the National Asset Database, and use such database in the development, coordination, integration, and implementation of plans and programs, including to identify, catalog, prioritize, and protect critical infrastructure and key resources in accordance with *Homeland Security Presidential Directive-7*, and in cooperation with all levels of government and private sector entities that the Secretary considers appropriate; and

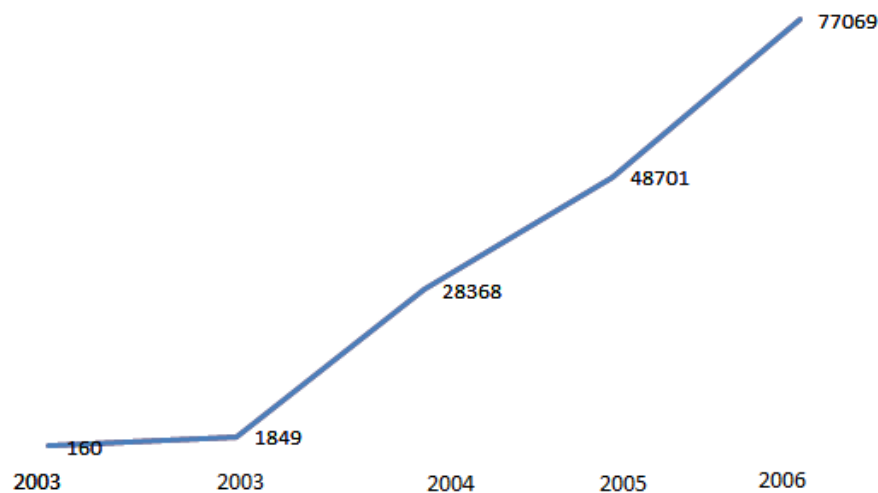
⁶⁴ Office of Inspector General, *Progress in Developing the National Asset Database*.

⁶⁵ United States Congress, *Committee Reports 109th Congress (2005–2006) House Report 109-713—Part 1* (Washington, DC: The Library of Congress, Thomas, 2007), http://thomas.loc.gov/cgi-bin/cpquery/?&sid=cp109alJsu&r_n=hr713p1.109&dbname=cp109&&sel=TOC_192496&.

(B) Consulting the National Asset Database, along with other appropriate resources, in providing any covered grant to assist in preventing, reducing, mitigating, or responding to a terrorist attack.⁶⁶

The Authorization Act also tasked the DHS Secretary to provide an annual report of the “extent to which the database has been used as a tool for allocating funds to prevent, reduce, mitigate, and respond to terrorist attacks.”⁶⁷ According to the DHS Office of Inspector General’s (OIG’s) report *Progress in Developing the National Asset Database*, 77,069 critical assets were designated in 2006. See Figure 1.⁶⁸

Figure 1. National Asset Database Growth 2003–2006



From Office of Inspector General, *Progress in Developing the National Asset Database* (OIG-06-40) (Washington, DC: Department of Homeland Security, 2006), http://www.oig.dhs.gov/assets/Mgmt/OIG_06-40_Jun06.pdf.

CF and government facilities account for nearly 40% of the nationally designated critical facilities. The original criteria for the July 2004 DHS data call provided the guidance for identifying facilities as CI quantified critical CF as “commercial centers with potential economic loss impact of \$10 billion or capacity of more than 35,000

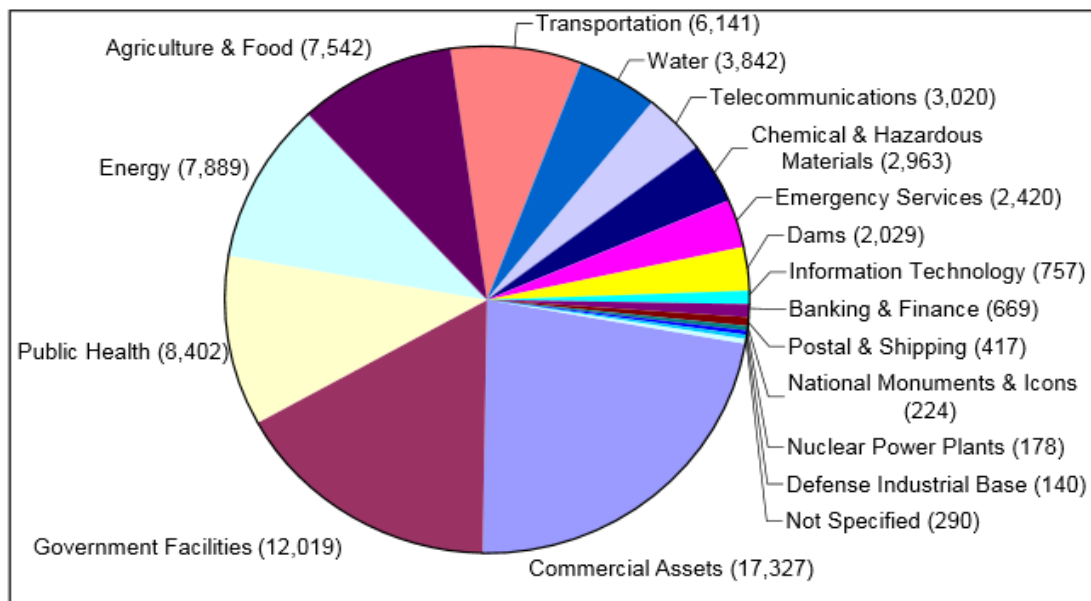
⁶⁶ United States Congress, *Committee Reports 109th Congress (2005–2006) House Report 109-713—Part 1*

⁶⁷ Ibid.

⁶⁸ Office of Inspector General, *Progress in Developing the National Asset Database*.

individuals.” While those numbers may seem significant, \$10 billion dollars in losses is not nationally significant in a \$2.4 trillion economy,⁶⁹ and 128 different universities have division football programs playing in stadiums with capacities over 35,000 individuals.⁷⁰ It seems unlikely that the football stadium at every large university is an infrastructure facility that is essential to the nation. These broad criteria for the NADB likely were the reason the number of critical facilities grew so rapidly. See Figure 2.

Figure 2. National Asset Database Totals by Sector



From Office of Inspector General, *Progress in Developing the National Asset Database* (OIG-06-40) (Washington, DC: Department of Homeland Security, 2006), http://www.oig.dhs.gov/assets/Mgmt/OIG_06-40_Jun06.pdf.

The DHS Inspector General concluded that the NADB contained “many unusual or out-of-place assets whose criticality is not readily apparent, and too few assets in essential areas and may represent an incomplete picture.” The assets in question included “4,055 malls, shopping centers, and retail outlets, 224 racetracks, 539 theme parks and 163 water parks, 1,305 casinos, 234 retail stores, 514 religious meeting places, 127 gas

⁶⁹ “Current United States GDP,” 2015, <http://data.worldbank.org/indicator/NY.GDP.MKTP.CD>.

⁷⁰ “Current NCAA Division 1 Football Teams,” 2010, <http://www.databasefootball.com/College/teams/teamlist.htm>.

stations, 130 libraries, 4,164 educational facilities, 217 railroad bridges, and 335 petroleum pipelines.”⁷¹

How did DHS end up with so many facilities on the NADB list? The broad scope of the IP mission, selection criteria that are below the threshold for national significant, a \$4 billion annual program budget that needed to be spent, and lack of measureable criteria of assessing risk, protection, and performance, were likely contributing factors to the problem. Another likely source of the problem is the reliance of DHS on facilities to self-assess risk.

B. OVERESTIMATION OF RISK DURING VULNERABILITY ASSESSMENTS OF FACILITIES

The September 2014 United States GAO *Report to Congressional Requesters—Critical Infrastructure Protection: DHS Action Needed to Enhance Integration and Coordination of Vulnerability Assessment Efforts* provides a laundry list of issues the department is having with assessing and documenting risks to CI facilities. DHS has “not consistently captured and maintained data, is not positioned to manage an integrated and coordinated government approach for assessments called for in the NIPP, and current efforts potentially are potentially duplicative or leave gaps among the CI [facilities] assessed.”⁷²

It should be noted that while a wide variety of risks arise from natural disasters and Internet-based cyber disruptions, the DHS assessments focus on physical vulnerabilities to a terrorist attack on a facility that can be lessened by protective measures including the presence of a security force, access control, or perimeter barriers.⁷³ Of the 10 DHS vulnerability assessment tools, all 10 have questions relating to vulnerability to intentional attacks but only two of the 10 have assessment criteria

⁷¹ John Moteff, *Critical Infrastructure: The National Asset Database* (CRS Report Order Code RL33648) (Washington, DC: Congressional Research Service, 2007), 1–7.

⁷² Government Accountability Office, *Critical Infrastructure Protection DHS Action Needed to Enhance Integration and Coordination of Vulnerability Assessment Efforts*.

⁷³ *Ibid.*, 4.

relating to “vulnerability to all-hazards,” such as hurricanes and earthquakes.⁷⁴ See Figure 3.

Figure 3. GAO Comparison of Selected Areas Included in the Department of Homeland Security Vulnerability Assessment Tools and Methods

DHS component	Assessment tool or method									
	National Protection and Programs Directorate				Transportation Security Administration				U.S. Coast Guard	
Area	Infrastructure Survey Tool	Site Assistance Visit	Chemical Security Assessment Tool	Security Vulnerability Assessment	Modified Infrastructure Survey Tool	Joint Vulnerability Assessment	Baseline Assessment for Security Enhancements	Pipeline Security Critical Facility Security Review	Freight Rail Risk Analysis Tool	Port Security Assessment
Vulnerabilities to intentional acts	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Vulnerabilities to all hazards	✓	✓								
Resilience management	✓	✓	✓			✓	✓	✓	✓	✓
Security force	✓	✓	✓	✓	✓	✓	✓		✓	✓
Perimeter security	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Entry controls	✓	✓	✓	✓	✓	✓	✓		✓	✓
Electronic security systems	✓	✓	✓	✓	✓	✓	✓		✓	✓
Utility systems/providers/dependencies identified	✓	✓	✓	✓	✓	✓	✓		✓	✓
Cybersecurity	✓	✓	✓	✓	✓	✓				
Inventory controls/measures	✓	✓	✓	✓		✓	✓			✓

Source: GAO analysis of DHS documents. | GAO-14-507

From Government Accountability Office, *Critical Infrastructure Protection DHS Action Needed to Enhance Integration and Coordination of Vulnerability Assessment Efforts* (GAO-14-507) (Washington, DC: U.S. Government Accountability Office, 2014), 19, <http://www.gao.gov/assets/670/665788.pdf>.

The Homeland Security Act of 2002 required DHS to conduct vulnerability assessments to assess and prioritize CI facilities. The GAO found that between 2011 and 2013, DHS conducted thousands of vulnerability assessments but the department is not equipped to integrate the various assessments to identify priorities.⁷⁵ With more than 70,000 CI facilities across the country, DHS also relies on facilities to self-assess risk with tools, such as the DHS IP Risk Self-Assessment Tool, which relies on the facility

⁷⁴ Government Accountability Office, *Critical Infrastructure Protection DHS Action Needed to Enhance Integration and Coordination of Vulnerability Assessment Efforts*, 18.

⁷⁵ Government Accountability Office, *Critical Infrastructure Protection DHS Action Needed to Enhance Integration and Coordination of Vulnerability Assessment Efforts*.

operator to decide the threat rating, vulnerability, hazards, and vulnerabilities.⁷⁶ Between October 2010 and September 2014, GAO found that facility operators submitted 7,600 self-assessments of facilities to DHS.⁷⁷ The Environmental Protection Agency offers the Vulnerability Self-Assessment Tool (VSAT) 6.0 to allow water and wastewater facilities to determine quantitative risk and resilience metrics, asset prioritization, and threats.⁷⁸ Unfortunately, people are generally very poor at self-assessing.

People are generally over optimistic and overconfident with self-assessments. Poor self-assessment skills also apply to people with specialized knowledge who should be well qualified to make informed decisions. In an experiment with Masters of Business Administration (MBA) students (who have knowledge of statistics and standard distribution), a group was asked to predict the final grades in the course. With a standard distribution, 50% will be above and below the average with only 10% in the top decile. The results of the survey showed that a majority of students placed themselves in the highest or second highest decile, and only 5% placed themselves in the bottom 50%.⁷⁹ Even a group of students who should be well informed about standard distribution of grades, completely failed to predict their performance accurately in a course that shows the weakness in people's self-assessment skills. This phenomenon of poor assessment is known as the "optimism bias."

The optimism bias extends beyond MBA students. People under estimate their risk for car accidents, think the chances of divorce are low, and expect to receive future promotions, gain wealth beyond current means, and possess a superior intellect to

⁷⁶ Department of Homeland Security, *Commercial Facilities Risk Self-Assessment Tool* (Washington, DC: Department of Homeland Security, 2012), http://www.ahla.com/uploadedFiles/RSAT%20Fact%20Sheet_05172012.pdf.

⁷⁷ Government Accountability Office, *Critical Infrastructure Protection DHS Action Needed to Enhance Integration and Coordination of Vulnerability Assessment Efforts*, 13.

⁷⁸ "Vulnerability Self Assessment Tool (VSAT) 6.0," September 4, 2014, <http://water.epa.gov/infrastructure/watersecurity/techtools/vsat.cfm>.

⁷⁹ Richard H. Thale and Cass R. Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness* (New Haven, CT: Yale University Press, 2008), 20.

others.⁸⁰ Optimism bias is evident in compulsive gamblers who will consistently overestimate the probability of winning high-risk bets.⁸¹

The DHS Critical Infrastructure Protection Program hinges on assessing the risks and vulnerabilities to infrastructure facilities and prioritizing the protection of the most vulnerable ones. It creates an incentivized system in which the facilities that are determined to have the highest risk become the facilities with the most resources (and considered to be the most important). Just as an MBA student has a personal desire to receive a high grade or a gambler is motivated by a reward, a facilities manager conducting a risk self-assessment will likely be subconsciously biased to assess greater risks than actually exist. This problem can be exacerbated by inconsistent methods of assessing and documenting risk. DHS provides 10 different risk assessment tools that each vary in length, depth, and content as show in Table 3 from the GAO report that is presented in Figure 4.

⁸⁰ Tali Sharot, “The Optimism Bias,” *Science Direct*, 21, no. 23 (2011): R941–R945, <http://www.sciencedirect.com/science/article/pii/S0960982211011912>.

⁸¹ “Pathological Gambling Caused by Excessive Optimism,” April 29, 2013, <http://www.sciencedaily.com/releases/2013/04/130429102400.htm>.

Figure 4. Length of Department of Homeland Security Vulnerability Assessment Tolls and Methods (Number of Pages and Questions), by Type

Vulnerability assessment tool or method	DHS office or component	Number of pages	Minimum number of questions
Infrastructure Survey Tool (IST)	National Protection and Programs Directorate (NPPD)	296	More than 100 ^a
Site Assistance Visit (SAV)	NPPD	253	More than 100 ^a
Chemical Security Assessment Tool Security Vulnerability Assessment (CSAT SVA)	NPPD	107	More than 100 ^a
Modified Infrastructure Survey Tool (MIST)	NPPD	165	More than 100 ^a
Joint Vulnerability Assessment (JVA)	Transportation Security Administration (TSA)	57 ^b	More than 100 ^a
Baseline Assessment for Security Enhancements (BASE)	TSA	14	205
Pipeline Security Critical Facility Security Review (CFSR)	TSA	21	166
Freight Rail Risk Analysis Tool	TSA	1	17
Port Security Assessment ^c	Coast Guard	5 ^d	16
Maritime Transportation Security Act (MTSA) ^e	Coast Guard	Not applicable	Not applicable

Source: GAO analysis of DHS documents. | GAO-14-507

From Government Accountability Office, Critical Infrastructure Protection DHS Action Needed to Enhance Integration and Coordination of Vulnerability Assessment Efforts (GAO-14-507) (Washington, DC: U.S. Government Accountability Office, 2014), 17, <http://www.gao.gov/assets/670/665788.pdf>.

An objective method for assessment should remove as many subjective measures as possible, but the GAO report found “differences in the detail of information collected in individual areas making it difficult to determine the extent to which the information collected was comparable [to other facilities] and what assumptions or judgments were used while gathering assessment data.”⁸² Some risk assessment tools use “yes/no” questions, while others have drop down menus of options and open-ended narratives.

⁸² Government Accountability Office, *Critical Infrastructure Protection DHS Action Needed to Enhance Integration and Coordination of Vulnerability Assessment Efforts*, 20.

Once a facility is designated as a “critical infrastructure,” or receives resources from the government, the facility manager is likely to become “loss adverse” to giving up those resources or the prestige of the designation when conducting future risk assessments. Along the lines of being adverse to loss, people will disproportionately decide to stick with a current decision rather than make a change. People will stay with a retirement plan or health care policy even if more attractive alternatives are available, and this same thinking likely applies to a facility manager determining risks and vulnerabilities to a facility.⁸³ The “status quo bias” may contribute to a facility that has been assessed as having a risk or vulnerability, reporting that same high level of risk in future assessments even if the risk or vulnerability has actually decreased.⁸⁴

While it is unrealistic for DHS to assess all CI facilities, the lack of consistency in self-assessment tools and the likelihood for errors in self-assessment creates unreliable results. The problem is compounded because GAO found that “it is unclear what areas DHS believes should be included in a comprehensive vulnerability assessment.” GAO reports, “DHS is not in a position to integrate assessments conducted or required by components within DHS to identify priorities for protective and supportive measures regarding threats to the nation or to support national-level comparative risk assessments.”⁸⁵

C. LOTS OF MONEY AND FEW MEASURABLE RESULTS

The 2014 *National Protection Framework*⁸⁶ defined CI protection as

protecting the physical and cyber elements of critical infrastructure. This includes actions to deter the threat, reduce vulnerabilities, or minimize the consequences associated with a terrorist attack, natural disaster, or

⁸³ William Samuelson and Richard Zeckhauser, “Status Quo Bias in Decision Making,” *Journal of Risk and Uncertainty* 1 (1988): 7–59. <http://www.hks.harvard.edu/fs/rzeckhau/SQBDM.pdf>.

⁸⁴ Thale and Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness*, 34.

⁸⁵ Government Accountability Office, *Critical Infrastructure Protection DHS Action Needed to Enhance Integration and Coordination of Vulnerability Assessment Efforts*, 24.

⁸⁶ Federal Emergency Management Agency, *National Protection Framework First Edition* (Washington, DC: Department of Homeland Security, 2014), http://www.fema.gov/media-library-data/1406717583765-996837bf788e20e977eb5079f4|174240/FINAL_National_Protection_Framework_20140729.pdf.

manmade disaster. Critical Infrastructure Protection is an element of critical infrastructure security and resilience as detailed in *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience*.⁸⁷

While the mission is defined, the goals of the mission remain unclear. The 2013 *National Infrastructure Protection Plan Supplemental Tool* states, “goals and objectives are likely to vary across sectors and organizations depending on the risk landscape, operating environment, and composition of a specific industry, resource, or other aspect of critical infrastructure.”⁸⁸

Even with undefined goals, IP is a \$72 billion market that is expected to double to \$114 billion by 2019 according to a *Security Technology* market analysis prediction.⁸⁹ The DHS National Protection and Programs Director was budgeted \$2.5 billion in 2013 with additional resources for IP also included in FEMA’s \$10.6 billion, FEMA Grants Program’s \$2.3 billion, and DHS Science & Technology’s \$668 million budgets.⁹⁰ All this funding equates to an enormous amount of federal resources being dedicated to the CI protection mission, as shown in Figure 5.

⁸⁷ Federal Emergency Management Agency, *National Protection Framework First Edition*, 9.

⁸⁸ Federal Emergency Management Agency, *National Protection Framework First Edition*.

⁸⁹ “Press Release: Critical Infrastructure Protection Market Worth \$ 114.30 Billion by 2019,” 2015, <http://www.marketsandmarkets.com/PressReleases/critical-infrastructure-protection-cip.asp>.

⁹⁰ Department of Homeland Security, *FY 2013 Budget in Brief* (Washington, DC: Department of Homeland Security, 2013), <http://www.dhs.gov/xlibrary/assets/mgmt/dhs-budget-in-brief-fy2013.pdf>.

Figure 5. Funding for the Infrastructure Protection and Information Security Program (in millions of dollars)

Program Project Activity	FY2013 Enacted (pre- sequester)	FY2014 Request	FY2014 House Passed	FY2014 Senate Reported	P.L. 113-76
Infrastructure Protection	\$260	\$261	\$261	\$273	\$263
Identification, Analysis, and Planning	59	58	66	66	63
Sector Management and Governance	67	60	60	65	63
Regional Field Operations	56	57	57	57	57
Infrastructure Security Compliance	78	86	77	86	81
Cybersecurity	756	810	786	804	792
Cybersecurity Coordination	4	4	4	4	4
US-CERT Operations	93	103	102	102	102
Federal Network Security	236	200	200	200	200
Network Security Deployment	329	406	382	393	382
Global Cybersecurity Management	26	19	19	26	26
Critical Infrastructure Cyber Protection and Awareness	63	73	73	73	73
Business Operations	6	5	5	5	5
Communications	140	131	130	132	131
Office of Emergency Communications	39	37	36	38	37
Priority Telecommunications Services	53	53	53	53	53
Next Generation Networks	24	21	21	21	21
Programs to Study and Enhance Telecommunications	13	10	10	10	10
Critical Infrastructure Protection	11	9	9	9	9
Total, Infrastructure Protection and Information Security	1,158	1,202	1,177	1,209	1,187

Source: CRS analysis of P.L. 113-6, its accompanying Senate explanatory statement, P.L. 113-2, the FY2014 DHS Congressional Budget Justifications, H.R. 2217, H.Rept. 113-91 and S.Rept. 113-77, and Explanatory Text for H.R. 3547, Division F.

From John D. Moteff, *Critical Infrastructures: Background, Policy, and Implementation* (CRS Report No. RL30153) (Washington, DC: Congressional Research Service, 2015), <https://www.fas.org/sgp/crs/homesecc/RL30153.pdf>.

In response to 2006 and 2011 efforts by Congress and GAO to determine the cost-benefit of current CI protection programs, GAO issued the 2013 report *Critical Infrastructure: Assessment of the Department of Homeland Security's Report on the*

*Results of Its Critical Infrastructure Partnership Streamlining Efforts.*⁹¹ According to the report:

In 2011, a report of the Senate Committee on Appropriations accompanying H.R. 2017—the fiscal year 2012 spending bill for DHS— noted that the department’s budget request stated that NPPD would streamline various methods and processes for coordination and information sharing with industry partners through NIPP management, Critical Infrastructure and Key Resources coordination, and SSA management. The committee report directed NPPD to provide a report, not later than 60 days after enactment of the bill, on the results from a thorough review of all efforts related to five areas: (1) coordinating and executing plans; (2) implementing performance metrics; (3) sustaining systemic communication; (4) executing SSA functions; and (5) providing education, training, and outreach. The committee report further stated that GAO shall review the results of the NPPD report and related efforts of the streamlining process no later than 60 days after receiving the report to determine the extent to which NPPD’s efforts were designed to ensure mission clarity, useful and actionable work products, efficacy of planning and information sharing, and that cost savings were achieved where possible.

As these initiatives are under way or planned, we could not assess the extent to which they will identify efforts to streamline the processes for coordination and information sharing with industry partners.

Figure 6 describes the requests of GAO for establishing streamlined practices being completed by DHS.

⁹¹ Government Accountability Office, *Critical Infrastructure: Assessment of the Department of Homeland Security’s Results of Its Critical Infrastructure Partnership Streamlining Efforts* (GAO-14-100R) (Washington, DC: U.S. Government Accountability Office, 2013), <http://www.gao.gov/assets/660/659074.pdf>.

Figure 6. DHS's Response to the Mandate in Each of the Five Areas Outlined in the Senate Committee Report

Area noted in Senate committee report	Summary of response	Response provided with respect to streamlining
Coordinating and Executing Plans	According to DHS's response, NPPD's Office of Infrastructure Protection (NPPD/IP) coordinates and executes plans with various stakeholders (e.g., CI owners and operators). DHS stated that the Critical Infrastructure Risk Management Enhancement Initiative (CIRMEI) seeks to ensure that activities conducted to meet the requirements of the NIPP are developed and executed considering foreseeable risks to critical infrastructure. DHS further reported that, as part of CIRMEI, DHS intends to develop short-term and long-term steps that NIPP partners can take to address certain risks and opportunities related to CI that are to enhance the coordination and execution of risk-management plans.	No
Implementing Performance Metrics	DHS's response stated that, as part of CIRMEI, outcome-based metrics were developed and implemented to better assess the current state of critical infrastructure protection and resilience. DHS highlighted a number of these metrics and related outcomes, and noted that there is much work to be done in defining a set of metrics against which all partners and NPPD/IP can measure progress in critical infrastructure protection and resilience.	No
Sustaining Systemic Communication	DHS reported that partnership, programmatic, and information sharing mechanisms are in place to provide systemic communication with and among CI stakeholders. To demonstrate that these mechanisms are in place, DHS noted, for example, the number of public and private members in the NIPP Sector Partnership and the number of fusion centers that joined the Critical Infrastructure Information Sharing Environment.	No
Executing Sector-Specific Agency Functions	According to DHS's response, SSAs function through five primary program areas: effective planning and activity integration, education and training, information sharing and communication, exercises, and assessment and mitigation. DHS highlighted performance metrics that NPPD uses to evaluate SSA functions. For example, NPPD maintains a metric to assess whether stakeholders have an understanding of critical infrastructure risks and interdependencies. According to DHS, NPPD analyses found that stakeholders understand that critical infrastructure risks and interdependencies exist, but further assessment is needed to understand the extent of the stakeholders' understanding.	No
Area noted in Senate committee report	Summary of response	Response provided with respect to streamlining
Providing Education, Training and Outreach	DHS stated that NPPD/IP offers a variety of education and training resources to CI stakeholders. For example, DHS reported that in 2011, the critical infrastructure information sharing environment hosted 28 educational events and reached approximately 17,500 stakeholders. DHS also stated that NPPD/IP conducts outreach to share information and intelligence, develop partnerships, and conduct vulnerability and security assessments, among other things. DHS's response also noted that the successful implementation of the NIPP partnership framework, for example, demonstrates the value of NPPD/IP outreach efforts.	No

Source: GAO analysis of DHS information.

From Government Accountability Office, Critical Infrastructure: Assessment of the Department of Homeland Security's Results of Its Critical Infrastructure Partnership Streamlining Efforts (GAO-14-100R), (Washington, DC: U.S. Government Accountability Office, 2013), <http://www.gao.gov/assets/660/659074.pdf>.

The failure to answer these Congressional and GAO inquiries follows a long line of similar shortfalls in providing evidence of program effectiveness and an overall lack of transparency by DHS. In response to GAO, the *DHS Critical Infrastructure Protection Cost-Benefit Report*⁹² is inconsistent regarding if cost-benefit analysis of CI protection has been undertaken. The GAO assessment did not have the scope to assess if measures to protect infrastructure were effective, or cost-effective, and DHS officials stated that by the time of the report, the information was outdated due to program maturation.

According to Senator Coburn's 2011 report on the effectiveness of DHS's CI protection efforts,

the Appropriations Committees of the Congress instructed DHS to review its efforts to streamline processes for coordinating and sharing information with private sector partners, including owners and operators of critical infrastructure, and to report on these efforts to Congress within 60 days. Two years later, the Appropriations Committees' request was answered with a report from DHS. GAO reviewed the report and found it did not discuss NPPD's effort to streamline the process for coordination and information sharing with industry partners, raising questions about whether the Department of Homeland Security was responding to Congress and making progress in this respect to become a more efficient partner with the private sector.⁹³

D. CHANGES TO NATIONAL CRITICAL INFRASTRUCTURE PRIORITIZATION PROGRAM

In 2013, GAO reported that the DHS Office of Infrastructure Protection shifted the priorities of the National Critical Infrastructure Protection Program (NCIPP) to focus efforts on three primary goals of identifying infrastructure that could significantly impact the nation, increase accuracy in prioritization, and improve planning and coordination with public and private stakeholders.⁹⁴ The updated list of facilities on the NCIPP would

⁹² Government Accountability Office, *The Department of Homeland Security's Critical Infrastructure Protection Cost-Benefit Report* (GAO-09-654R) (Washington, DC: U.S. Government Accountability Office, 2009), <http://www.gao.gov/new.items/d09654r.pdf>.

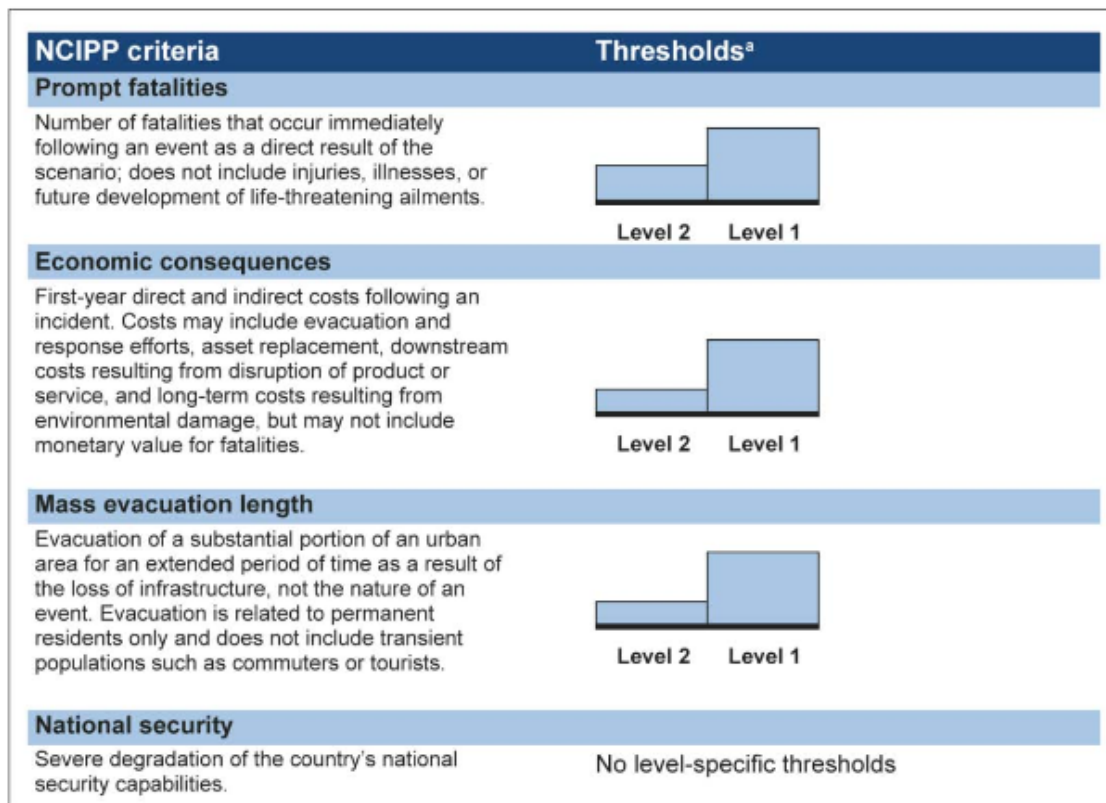
⁹³ Tom Coburn, *A Review of the Department of Homeland Security's Missions and Performance* (Washington, DC: United States Senate, 2015), 29, <http://www.hsgac.senate.gov/download/?id=B92B8382>

⁹⁴ Government Accountability Office, *Critical Infrastructure Protection—DHS List of Priority Assets Needs to be Validated and Reported to Congress* (GAO-13-296) (Washington, DC: U.S. Government Accountability Office, 2013), 9, <http://www.gao.gov/assets/660/653300.pdf>.

be used to allocate grant funding, prioritize protection programs, and inform incident planning and response efforts around the facilities.⁹⁵ Unfortunately, according to GAO, the changes to the composition of the prioritization list were not validated, and DHS did not establish a process for identifying the impacts of the changes.⁹⁶

The consequence-based criteria for determining the prioritization of a facility is based on immediate loss of life, economic consequences directly or indirectly occurring from the loss, or how the infrastructure impacts mass evacuations from urban areas (see Figure 7).

Figure 7. NCIPP Consequence-Based Criteria and Relative Threshold Levels



From Government Accountability Office, *Critical Infrastructure Protection—DHS List of Priority Assets Needs to be Validated and Reported to Congress* (GAO-13-296) (Washington, DC: U.S. Government Accountability Office, 2013), 14, <http://www.gao.gov/assets/660/653300.pdf>.

⁹⁵ Government Accountability Office, *Critical Infrastructure Protection—DHS List of Priority Assets Needs to be Validated and Reported to Congress*, 11.

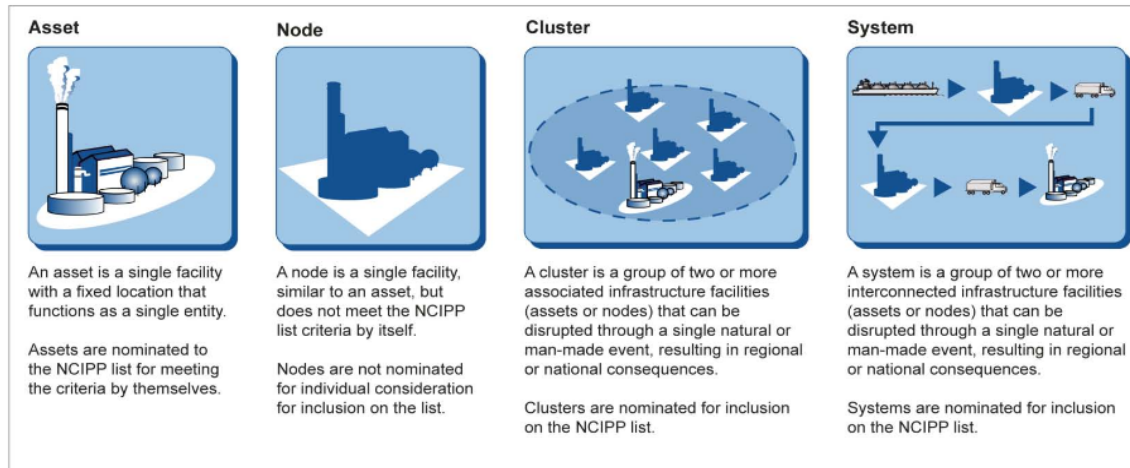
⁹⁶ Ibid., 12.

Just as the NADB focused on individual facilities instead of points of failure within the interconnected infrastructure system, the thresholds for prioritizing infrastructure in the NCIPP are also based around individual facilities losses with a focus on mass gatherings of people. The number of fatalities occurring immediately following an event suggests that something is happening at a facility that holds a large number of people. The future human losses from the destruction of a larger infrastructure system providing essential services are discounted from the prioritization criteria, which show the emphasis on single facilities. The measures of economic impact and evacuation time also align more closely with large facilities like stadiums and arenas instead of infrastructure systems, such as power grid components. It is unlikely that a power substation would have mass fatalities at the site, cause direct economic losses, or have an impact on evacuations but all those factors would be relevant if 80,000 people were in attendance at a football stadium.

While the NADB was a list of only individual facilities, the NCIPP differentiates between individual facilities (assets) and clusters or systems (groups of facilities). The 2013 *DHS National Infrastructure Plan Supplemental Tool* defines critical nodes as the point “where potential consequences would be highest”⁹⁷ but based on the GAO analysis (Figure 8), nodes are only included within the NCIPP list as groups of nodes. The factors that differentiate between single facilities that are assets and single facilities that are nodes are unclear.

⁹⁷ Department of Homeland Security, *Supplemental Tool: Executing a Critical Infrastructure Risk Management Approach* (Washington, DC: Department of Homeland Security, 2013), http://www.dhs.gov/sites/default/files/publications/NIPP%202013%20Supplement_Executing%20a%20CI%20Risk%20Mgmt%20Approach_508.pdf.

Figure 8. Description and Illustration of an Asset, a Node, a Cluster, and a System



From Government Accountability Office, *Critical Infrastructure Protection—DHS List of Priority Assets Needs to be Validated and Reported to Congress* (GAO-13-296) (Washington, DC: U.S. Government Accountability Office, 2013), 18, <http://www.gao.gov/assets/660/653300.pdf>.

GAO found that shifting the prioritization and designation of infrastructure “could hinder the ability to compare infrastructure across sectors and is not a validated process to ensure that it accurately reflects the nation’s highest-priority infrastructure.”⁹⁸ Using measures associated with large groups of people to evaluate the thresholds for importance of functional systems may not be an effective strategy. GAO reported, “DHS could not provide documentation explaining how the threshold levels were established and the NCIPP list had not been verified or validated by an external peer review.”⁹⁹

Regardless of if DHS is maintaining a national database of facilities or a national prioritization list, the criteria, and process for determining which infrastructure facilities or systems are nationally significant, has been an ineffective effort.

⁹⁸ Government Accountability Office, *Critical Infrastructure Protection—DHS List of Priority Assets Needs to be Validated and Reported to Congress*, 24.

⁹⁹ *Ibid.*, 25.

E. EXAMPLE OF THE PROBLEM: CRITICAL INFRASTRUCTURE CHEMICAL SECTOR

One example of the IP problem is the DHS CI chemical sector where DHS has dedicated 242-fulltime positions and approximately \$90 million to protecting 3,495 critical chemical sector facilities. Further complicating this issue, DHS has identified 40,000 total chemical facilities as critical but only 3,495 facilities have been categorized into tiers (measures of importance)¹⁰⁰ and have completed approved facility security plans.¹⁰¹ A significant amount of manpower and funding has been committed by DHS for assessing and protecting chemical facilities. Even with a \$90 million budget, only 10% of the facilities deemed to be critical have been assessed, which likely means the scope of the chemical sector protection mission is too broad. See Figure 9.

Figure 9. Number and Percentage of Facilities Assigned a Final Tier as of January 2013

	Number	Percent
Tier 1	117	3.4
Tier 2	406	11.6
Tier 3	1,040	29.8
Tier 4	1,932	55.3
Total	3,495	100.0

Source: GAO analysis of Infrastructure Security Compliance Division data.

From Government Accountability Office, *Critical Infrastructure Protection—DHS Efforts to Assess Chemical Security Risk and Gather Feedback on Facility Outreach Can Be Strengthened* (GAO-13-353) (Washington, DC: U.S. Government Accountability Office, 2013), 9, <http://www.gao.gov/products/GAO-13-353>.

This expansive designation of “critical” for the chemical sector facilities comes primarily from the vulnerability of the facilities to theft of dangerous chemical materials and sabotage of the facility causing a chemical release. The tiered assessments are not based on how the chemicals produced by the facility provide essential services to other infrastructure sectors (e.g., chlorine production essential for water treatment in the

¹⁰⁰ Government Accountability Office, *Critical Infrastructure Protection—DHS Efforts to Assess Chemical Security Risk and Gather Feedback on Facility Outreach Can Be Strengthened* (GAO-13-353) (Washington, DC: U.S. Government Accountability Office, 2013), 29, <http://www.gao.gov/products/GAO-13-353>.

¹⁰¹ Ibid.

surrounding area). The assessment approach used to measure risk to chemical facilities is based instead on the level of interest a terrorist would have in attacking or infiltrating the facility to obtain chemical materials to utilize in an attack elsewhere. The protective services provided by DHS assisted facilities with developing facility security plans, which focused on a single facility and not how the sector delivers critical functions to the public or other infrastructure sectors.¹⁰² In 2007, DHS established the chemical facilities anti-terrorism standards as a requirement of the Department of Homeland Security Appropriations Act of 2007 to address the highest risk chemical facilities in the country.¹⁰³ While IP should be based around assessing chemical facilities support for the overall infrastructure functions essential to the nation, the assessment and protection of these facilities is measured by risk of theft and infiltration. See Figure 10 for a list of seven standards.

¹⁰² Government Accountability Office, *Critical Infrastructure Protection—DHS Efforts to Assess Chemical Security Risk and Gather Feedback on Facility Outreach Can Be Strengthened*, 7.

¹⁰³ Office of the Inspector General, *Effectiveness of the Infrastructure Security Compliance Division's Management Practices to Implement the Chemical Facility Anti-Terrorism Standards Program* (Washington, DC: Department of Homeland Security, 2013), 85, https://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-55_Mar13.pdf.

Figure 10. DHS Chemical Facilities Anti-Terrorism Standards Risk-based Performance Standards

Risk-Based Performance Standards		Descriptions
1	Restrict Area Perimeter	Secure and monitor the perimeter of the facility.
2	Secure Site Assets	Secure and monitor restricted areas or potentially critical targets within the facility.
3	Screen and Control Access	Control access to the facility and to restricted areas within the facility by screening and/or inspecting individuals and vehicles as they enter.
4	Deter, Detect, and Delay	Deter, detect, and delay an attack, creating sufficient time between detection of an attack and the point at which the attack becomes successful.
5	Shipping, Receipt, and Storage	Secure and monitor the shipping, receipt, and storage of hazardous materials for the facility.
6	Theft and Diversion	Deter theft or diversion of potentially dangerous chemicals.
7	Sabotage	Deter insider sabotage.

From Office of the Inspector General, *Effectiveness of the Infrastructure Security Compliance Division's Management Practices to Implement the Chemical Facility Anti-Terrorism Standards Program* (Washington, DC: Department of Homeland Security, 2013), 14, https://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-55_Mar13.pdf.

Each of these seven performance standards shown in Figure 10 (there are 18 total) for chemical facilities are related to physical security of the facility against attack, unauthorized access, sabotage, or theft of materials. None of the 18 standards relate to the functionality of the facility or the interdependencies with other facilities. Also, no standard relating to information sharing or coordination with other infrastructure facilities exists. The Chemical Facilities Anti-Terrorism Standards (CFATS) program within the DHS National Protection and Preparedness Director was allocated a \$93 million budget in 2012 for personnel costs, training, systems, and program support.¹⁰⁴ Even with a list of security criteria that only relate to the physical security of individual facilities, the DHS Office of the Inspector General found that “more than five years since the program was

¹⁰⁴ Office of the Inspector General, *Effectiveness of the Infrastructure Security Compliance Division's Management Practices to Implement the Chemical Facility Anti-Terrorism Standards Program*, 11.

created, almost \$443 million had been appropriated, and no facility has gone through the entire CFATS regulatory process.”¹⁰⁵

Facilities within the DHS CI chemical subsector serve as an example of facilities that have been designated as “critical” yet protective measures funded by DHS only pertain to physical security at individual facilities. Even with the very limited scope of protective measures that do not address infrastructure as an interconnected and interdependent system, DHS’s internal report found that no facility was even completing the entire CFATS evaluation process. None of these protective measures link back to the overarching concept of CI being facilities so essential that their destruction would cause cascading impacts across the entire nation.

F. POTENTIAL SOLUTION—REFINE CRITICAL INFRASTRUCTURE DESIGNATION CRITERIA

DHS is required to manage risks to CI by *NIPP*, *PPD-21*, and the Homeland Security Act of 2002 but “DHS is not positioned to manage an integrated and coordinated government-wide approach for CI vulnerability assessment activities as called for by the *NIPP*.”¹⁰⁶ A remedy for this problem is reducing the overall number of facilities across the 16 CI sectors. Numerous agencies and DHS components conduct infrastructure risk assessments and have IP missions that overlap because too many different facilities are categorized as critical. Removing the low-risk and non-critical facilities can simplify interagency coordination by reducing the total number of locations, tasks, and national-level assessments. The corrective actions recommended by GAO include refining vulnerability assessment tools, consistently collecting information, avoiding duplication, and facilitating information sharing.¹⁰⁷ Each of these goals would be easier to accomplish with a smaller number of CI facilities to assess.

¹⁰⁵ Office of the Inspector General, *Effectiveness of the Infrastructure Security Compliance Division’s Management Practices to Implement the Chemical Facility Anti-Terrorism Standards Program*, 13.

¹⁰⁶ Government Accountability Office, *Critical Infrastructure Protection DHS Action Needed to Enhance Integration and Coordination of Vulnerability Assessment Efforts*, 37.

¹⁰⁷ *Ibid.*, 43.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. WHAT IS THE SOURCE OF THE PROBLEM WITH CRITICAL INFRASTRUCTURE PROTECTION POLICY?

We must not start our thinking on war with the tools of war—with the airplanes, tanks, ships, and those who crew them. These tools are important and have their place, but they cannot be our starting point, nor can we allow ourselves to see them as the essence of war. Fighting is not the essence of war, nor even a desirable part of it. The real essence is doing what is necessary to make the enemy accept our objectives as his objectives.

— Colonel John A. Warden, *The Enemy as a System*¹⁰⁸

A. MILITARY THEORY AND TARGET SELECTION

The primary component of the DHS CI protection mission is protecting facilities from terrorist attacks stemming from the PPD-21 requirement to “reduce the risks to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or man-made disasters.”¹⁰⁹ To create a plan for the protection of critical facilities, the intentions of the enemy need to be understood. It is unlikely that a terrorist group operating in the United States has the capability to destroy a nationally significant infrastructure target that provides life-sustaining services at the national level (a RAND terrorism risk modeling report found negligible terrorism risk outside top eight Urban Areas Security Initiative (UASI) cities and 10-ton explosive as the least likely type of bombing attack¹¹⁰). These nationally significant facilities would be attractive targets for an enemy nation-state with ballistic missile and airpower capabilities but the DHS IP measure are also not designed around defense from military air attacks. The current terrorist threat comes from homegrown violent extremist and supporters of violent

¹⁰⁸ John A. Warden, “The Enemy As a System,” *AirPower Journal*, Spring 1995, http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/warden.htm.

¹⁰⁹ “What is Security and Resilience?” August 24, 2015, <http://www.dhs.gov/what-security-and-resilience>.

¹¹⁰ Henry Willis, *Terrorism Risk Modeling for Intelligence Analysis and Infrastructure Protection* (Santa Monica, CA: RAND Corporation, 2006), http://www.rand.org/content/dam/rand/pubs/technical_reports/2007/RAND_TR386.pdf.

extremist groups who are motivated to inflict mass casualties by killing and injuring as many people as possible in a location accessible to the public.¹¹¹ These individuals or small groups of individuals lack the intelligence, organizational coordination, manpower, and resources to conduct a strategic war campaign against nationally significant infrastructure targets.

The current CI protection mission is convoluted because protection efforts are based around two competing strategies, which are terror groups interested in inflicting mass casualty versus organized militaries (or well-equipped paramilitary organizations) conducting strategic operations with the intent to cripple the nation's most significant infrastructure systems. Current policies group these two different types of adversarial action into a single protection mission when they are distinctly different.

B. METHODS OF ATTACK

Different military strategies have been taught and utilized by the United States and other modern militaries. These types of attacks are based around differing strategic objectives, the ability to gather intelligence, military capabilities, and available resources.

1. Figures and Tables

The Air Corps Tactical School theory¹¹² states targeted strikes to specific facilities or functions can result in economic destruction would lead to social collapse and defeat of the enemy. Lt Col Peter Faber, an expert in strategic aerial warfare, theorizes targeted strikes provide the means to win a war in the following manner:

1. Modern nations rely on industrial and economic systems for production of weapons and supplies for their armed forces, for manufacture of products, and provision of services to sustain life. Disruption or paralysis of these systems undermines both the enemy's *capability* and *will* to fight.

¹¹¹ "Countering Violent Extremism," July 20, 2015, <http://www.dhs.gov/topic/countering-violent-extremism>.

¹¹² Howard D. Belote, "Warden and the Air Corps Tactical School—What Goes Around Comes Around," *AirPower Journal*, Fall 1999, <http://www.airpower.maxwell.af.mil/airchronicles/apj/apj99/fal99/belote.html>.

2. Industrial and economic systems contain critical points whose destruction will break down these systems if bombs can be delivered with adequate accuracy to do this.
3. Air strike forces can penetrate air defenses without unacceptable losses and destroy selected targets.
4. Proper selection of vital targets in the industrial/economic/social structure of an industrialized nation, and their subsequent destruction by air attack, can lead to fatal weakening of an industrialized enemy nation and to victory through air power.¹¹³

Winning a war by employing targeted strikes requires knowledge of the enemy's key systems, intelligence to select the critical points, forces capable of making the attack, and forces that can avoid unacceptable losses.¹¹⁴

2. Series Warfare

Unlike targeted strikes that are carried out with aircrafts, in series warfare, "a commander concentrates forces in order to prevail against a single vulnerable part of the enemy's forces. If the commander prevails, the army regroups forces and moves on to attack another point in the enemy's defense. While the attacking army regroups, the enemy army may counter attack or move to defend another position."¹¹⁵ This back and forth process is termed "serial warfare" because of the "subsequent maneuver and counter-maneuver, attack and counterattack, and movement and pause."¹¹⁶ Series warfare continues until either army does not have the capabilities or will to continue fighting.

3. Parallel Attack

A combination of targeted attacks and series warfare is the concept of parallel attacks against a wide array of essential systems. The most important element of the parallel attack is understanding the targets that hold the highest value to the enemy system. Once the system is understood, a strategy must be developed to damage or

¹¹³ Peter Faber, "Competing Theories of Airpower: A Language for Analysis," *AirPower Journal*, April 30, 1996, <http://www.airpower.maxwell.af.mil/%20airchronicles/presentation/faber.html>.

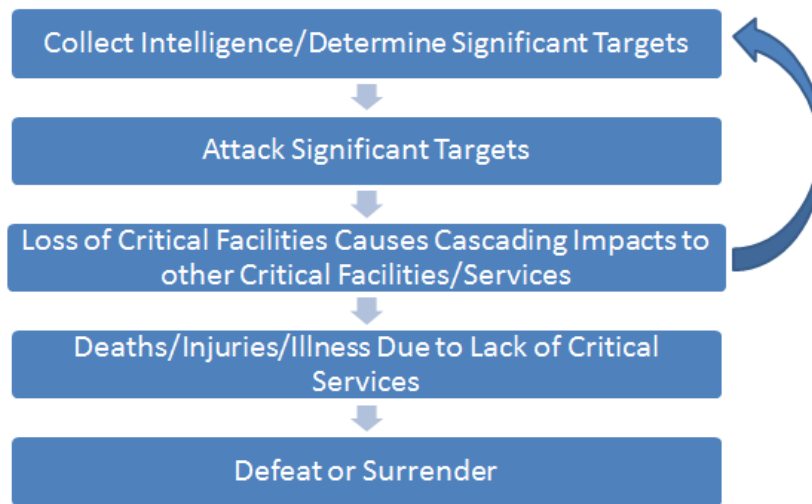
¹¹⁴ Ibid.

¹¹⁵ Ibid.

¹¹⁶ Warden, "The Enemy As a System."

paralyze it. A nation is likely to have a “small number of vital targets at the strategic level because most systems only cause localized disruptions if damaged.”¹¹⁷ The nationally significant targets “tend to be small, very expensive, have few backups, and are hard to repair”¹¹⁸ that aligns with the same concept of CI, which is interdependent systems that cause system-wide failures.

Figure 11. Process of Actions during Strategic Warfare



If a significant percentage of key targets are struck in parallel, the damage becomes insurmountable. The enemy can mitigate the effects of serial attacks by “dispersing the location of critical targets, by increasing the defenses of targets that are likely to be attacked, concentrating resources to repair damage to single targets, or conducting a counter offensive.”¹¹⁹ The purpose of the parallel attack is to deprive the enemy of the ability to respond effectively to mitigate the impacts of the attack. The higher the number of significant targets destroyed during each set of strikes, the higher the likelihood of debilitating the enemy.¹²⁰ The current DHS strategy of protecting CI by

¹¹⁷ Warden, “The Enemy As a System.”

¹¹⁸ Ibid.

¹¹⁹ Ibid.

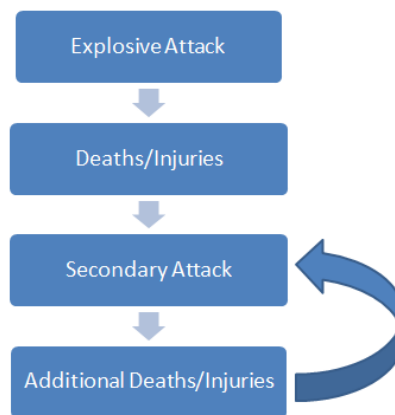
¹²⁰ Ibid.

adding redundancies and hardening targets directly relates to the concept of identifying and protecting key targets from the parallel attack.

4. Mass Casualty Attack

Online publications, such as The Islamic State's *Dabiq* and Al Qaeda's *Inspire*, have provided instructions for supporters to carry out homemade conventional explosive and small arms attacks. The intent of these attacks is to inflict as many deaths and injuries as possible by targeting crowded public areas and special events. An example of this tactic was the April 15, 2013 Boston Marathon bombing attack where two radicalized individuals produced small homemade explosives that were detonated at the crowded finish line area of the city's annual marathon.

Figure 12. Process of Actions Occurring during Conventional Terrorist Attacks



The likely purpose of these attacks on the American public was to kill and injure people to cause fear rather than being a focused strike on an infrastructure component that would result in cascading impacts to the systems that underpin the functions of the United States.

5. Mutually Assured Destruction

The underlying theory of nuclear war between multiple industrial nations with nuclear weapons is that if a nuclear weapon were detonated, mutually assured destruction

would occur to all nations involved due to counter nuclear attacks. In the end, nobody would win the nuclear war because the casualties and damage on every side would be catastrophic.

The mutually assured destruction (MAD) concept is applicable to planning for CI protection based on the size of an attack that would be required to damage a critical system. The massive amount (a theoretical 10,000 pounds or more of explosives exceeding the size of the Oklahoma City federal building attack) that would be needed to destroy a large dam or multiple simultaneous attacks on electrical power plants would be of scope large enough to assure the destruction of the nation-state, paramilitary army, or terrorist group responsible. Is it realistic to plan for, or protect against attacks, of this scope at infrastructure facilities when it is unlikely that terrorist groups could utilize such a large quantity of explosives? Increasing physical security at a facility with taller fences and stricter identification checks designed to stop a small-scale and unlikely terrorist attack would do nothing to protect against a ballistic missile strike, which is the most realistic, but very unlikely, threat to the facility.

C. WARDEN'S FIVE-RING SYSTEM THEORY

Countries are inverted pyramids that rest precariously on their strategic innards—their leadership, communications, key production, infrastructure, and population. If a country is paralyzed strategically, it is defeated and cannot sustain its fielded forces though they may be fully intact.

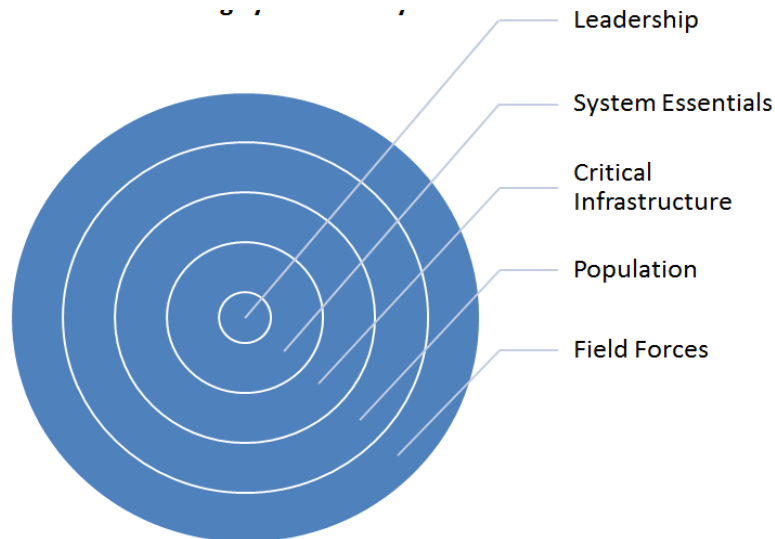
— Colonel John Warden, *Air Theory for the Twenty-First Century*¹²¹

Warden's five-ring system theory is a concentric ring concept of targeting the central rings that hold the highest strategic value (see Figure 13; the central ring is also the smallest target). In the rings beyond the highest value targets, the targets become larger and have less strategic significance. Warden selected five general systems that he

¹²¹ Anthony B. Carr, "America's Conditional Advantage: Airpower, Countering Urgency, and the Theory of John Warden," Homeland Security Digital Library, June 1, 2009, <https://www.hsdl.org/?view&did=697900>.

believed were key centers of gravity to exploit against any enemy (leadership, organic essentials,¹²² infrastructure, population, and fielded military forces).

Figure 13. Warden's Five-Ring System Theory



From Clayton Chun, "John Warden's Five Ring Model and the Indirect Approach to War," ETH Zurich, June 1, 2008, <http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&lng=en&id=57408>.

Warden's model provides a framework for how to defeat an enemy through destruction of critical components instead of engaging in combat with a conventional army.¹²³ This strategy is only effective if the attacker has the ability to identify and strategically plan how to destroy each of those systems in a specific order.¹²⁴ Warden's theory aligns with DHS's tiered approach to IP and the NADB. If military theorists trained in Warden's approach looked at how to identify and protect domestic infrastructure, they would likely think of it through a concentric ring-based system.

The flaw in applying Warden's theory to domestic IP is that the strategic values of the targets within each ring are not static. Leadership can be adaptive and resilient, the

¹²² Defined as "the facilities or processes without which the state or organization cannot maintain itself. It is not necessarily directly related to combat." Warden, "The Enemy As a System."

¹²³ Chun, "John Warden's Five Ring Model and the Indirect Approach to War."

¹²⁴ Ibid., 301.

relationships between systems can be too complex to understand completely, and most adversaries lack the resources necessary to conduct parallel attacks across a vast array of domestic targets.¹²⁵ These same problems are also evident in current CI protection policies because as facilities are hardened, demand for services changes, populations shift, different technologies are developed, and the criticality of infrastructure facilities also changes. Compounding the problem, the concentric ring system is ineffective if the wrong facilities are identified as being the key targets. Placing non-essential system into the central rings creates a large core rather than concentric rings that delineate the importance of different assets.

Warden's theory depends on taking a snapshot of the enemy system and carefully analyzing it to understand the weaknesses in the system. This same strategy is not an effective manner of analysis of vulnerabilities to domestic infrastructure over an extended period of time. Conducting assessments of infrastructure and creating tiered lists of resources would provide strategic planners with the critical systems at that point in time but as the value of targets changes, the target list would become less and less useful. The effectiveness of the target list would also be contingent on the how completely it captured the entirety of the system. Identifying individual facilities would only be useful if their destruction caused the cascading impacts that could cripple the essential functions of the enemy. The process of identifying these interdependencies would require an analysis of the entire system to determine the points of failure and then tracing the failures back to identify individual facilities as key targets. The current DHS policy identifies sectors of infrastructure and then identifies individual facilities within the separate sectors. This approach lacks the key "enemy as a system" concept of understanding the interdependencies and identifying the specific points of failure in the system. These points of failure are not broad sets of infrastructure systems; they are small areas of high strategic value in the center of the concentric rings.

¹²⁵ Ibid., 306.

D. TERRORISM DIFFERS FROM STRATEGIC WARFARE

The September 11, 2001 attacks on New York City and the Pentagon, the March 11, 2004 train bombings in Madrid, the July 7, 2005 London transit bombings, and the 2010 attempted Atlantic airline bombings with ink cartridges concealing explosives are all examples of how the most sophisticated terrorist attacks in recent history are different from strategic warfare.

These attacks were not targeted strikes against essential systems intended to cripple an enemy population. The Madrid¹²⁶ and London¹²⁷ attacks targeted transportation systems and occurred along busy transit pathways. However, the attacks did not target the key hubs of the system or cause cascading outages through the system. The same attacks carried out in more carefully selected locations could have caused wider impacts to the transportation system and inflicted a greater number of casualties. A strategic targeted strike intended to cripple transportation system would have occurred in a different manner.

The four major terrorist attacks also did not follow the concepts of series warfare in which an attack is mounted, resources are regrouped, and a subsequent attack occurs. Following the plane crashes at the WTC and the Pentagon, no plan or operation was in place for a second wave of attacks. If the 9/11 attacks were part of a series warfare strategy, a second operation would have already been underway but was not.¹²⁸ The same was true of the European transit bombings where coordinated attacks occurred but no second or third wave of subsequent attacks were prepared.

While the 9/11 attacks and the transit bombings targeted multiple locations, these attacks were not examples of a parallel attack strategy either. A parallel attack simultaneously strikes the key facilities in an area causing a crippling effect across the entire system. These significant terrorist attacks did not cripple the individual systems

¹²⁶ “Madrid Train Attacks: How the Attacks Happened,” <http://news.bbc.co.uk/2/shared/spl/hi/guides/457000/457031/html/default.stm>.

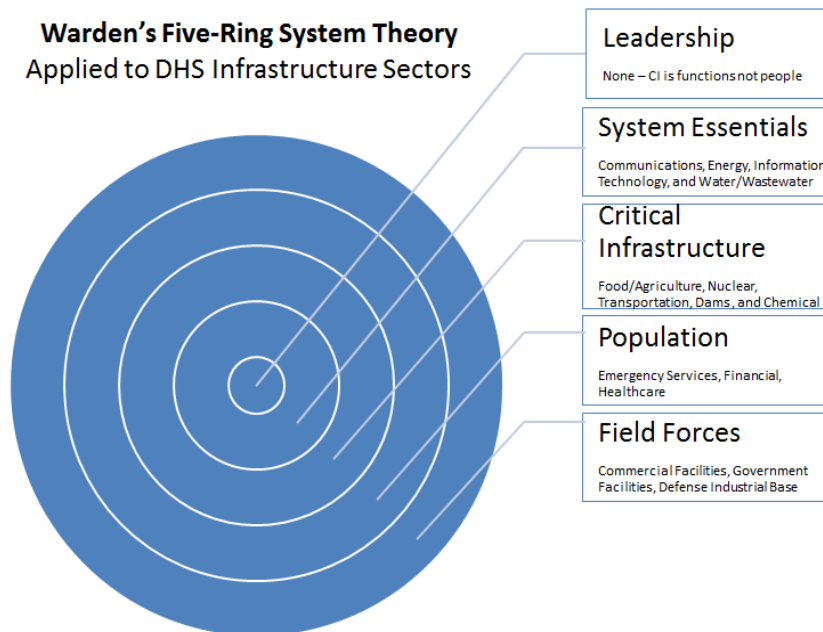
¹²⁷ “London Bombings Toll Rises to 37,” July 7, 2005, <http://news.bbc.co.uk/2/hi/uk/4661059.stm>.

¹²⁸ David Stout, “Original Plan for 9/11 Attacks Involved 10 Planes, Panel Says,” *The New York Times*, June 16, 2004, <http://www.nytimes.com/2004/06/16/politics/16CND-REPORT.html>.

that they targeted (e.g., striking the Pentagon did not shut down the U.S. military) or cause cascading impacts that crippled other essential systems. Each attack caused isolated impacts to a single component of the infrastructure system.

The timing and location of the 9/11 and transit attacks also demonstrate that the attacks were not intended to cause the maximum number of casualties possible. While 50,000 people worked in the original WTC towers, the attack occurred before 9:00 AM when most people get to work.¹²⁹ Instead of potentially killing 50,000 people, 2,977 people died when the plane struck at 8:46 AM.¹³⁰ Al Qaeda operatives spent years planning the 9/11 attack so it seems unlikely that they would have chosen to strike before 9:00 AM if the intent was to carry out a mass causality attack that would kill as many people as possible.

Figure 14. Warden’s Five-Ring System Theory Applied to DHS Critical Infrastructure Sectors



¹²⁹ “The World Trade Center—Facts and Figures,” accessed July 22, 2015, <https://www.nysm.nysed.gov/wtc/about/facts.html>.

¹³⁰ “September 11th Fast Facts,” March 27, 2015, <http://www.cnn.com/2013/07/27/us/september-11-anniversary-fast-facts/>.

Based on Warden's concentric rings theory, each of the terrorist attacks targeted the outermost rings that consist of the population and the field forces. If the terrorist attacks were strategic in nature, they would have likely tried to target the inner rings to cause more disruption across the entire country. Attacks targeting the inner rings could have been the New York Stock Exchange or the White House.

E. TERRORISTS HISTORICALLY DO NOT TARGET CRITICAL INFRASTRUCTURE

Improvised explosives, vehicle borne explosives, and firearms were the primary weapon in more than 99% of terrorist attacks according to the *Mineta Transportation Institute National Transportation Security Center of Excellence* study of multiple terrorism attack databases.¹³¹ While these types of attacks have the power to kill people and cause damage to property, they do not have the destructive capability to cease the functions of most CI facilities, such as power plants, telecommunications hubs, dams, water treatment facilities, regional transportation systems, and so on. Why is protection of facilities providing essential infrastructure functions a primary goal of DHS when these facilities are rarely targeted, and do not align with the motivation for terrorist groups?

Protecting CI against terrorist attacks is a primary mission of DHS, but the execution of this mission is flawed in many ways. Current policies and procedures look at targets in a different way than how a terrorist would select a target for attack. The protection of potential targets is designed around methods of attack that are different from how the majority of terrorist attacks are carried out. The consequences of an attack on a target are assessed based on the number of deaths, injuries, and dollars rather than the public exposure or alignment with an ideology that the target represents. Following similar ideas as the book, *From the Terrorist's Point of View*, rather than refine the approach to identify threats, current practice is to cast a larger and larger net, which requires greater resources for smaller results.

¹³¹ "Explosives and Incendiaries Used in Terrorist Attacks on Public Surface Transportation: A Preliminary Empirical Examination," March 1, 2010, <http://transweb.sjsu.edu/MTIportal/research/publications/documents/2875-IED-Support-Research.pdf>.

The mission of protecting CI can be refined through a psychological approach to evaluate why a terrorist attacks, a likely method of attack, and the type of target that would align with the desired results. Unlike convention warfare, terrorists view their tactics as a driver for social change making the highest value targets different from those chosen by a conventional army commander.

F. FEAR—THE CRITICAL STRATEGY OF TERRORISM

Terrorism experts like Bruce Hoffman argue that large-scale terrorist attacks with weapons of mass destruction (which have never occurred) and large events like the 9/11 attacks on the WTC are counter-productive strategies for terrorist groups. Small-scale attacks cause “disproportionately enormous consequences, generate fear and alarm, and thus serve the terrorists’ purposes just as well as a larger weapon or more ambitious attack.”¹³² According to Breckenridge and Zimbardo, “a heightened sense of crisis can lead to political disaffection and diminished confidence in the government”¹³³ and the resulting fear and anxiety across the population from the attack aligns better with terrorist’s goals of political or social changes than inflicting mass destruction or casualties. For example, Osama Bin Laden’s attack on the United States prior to September 11, 2001 were also attempting to erode public support and cause political pressure to remove U.S. forces from the Middle East. These attacks were intended to erode the general public’s support of U.S. leaders, not to kill the entire American population. “It is not surprising that fear and apprehension can have considerable political consequences. Affective influences on attention, memory, and judgment contribute to the widespread experience of disproportionate vulnerability and looming threat appraisal that make terrorism a more psychologically complex phenomenon.”¹³⁴

¹³² Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 2006), 8.

¹³³ Bruce Michael Bongar, *Psychology of Terrorism* (Oxford: Oxford University Press, 2007), 117.

¹³⁴ *Ibid.*, 118.

G. OSAMA BIN LADEN'S STRATEGY—OCCUPIED COUNTRY STRATEGY

While the conventional army wants to conquer territory at the lowest cost, Osama Bin Laden's strategy was the opposite. Instead of wanting to invade America and take over resources, his plan was to draw the United States into a prolonged and unwinnable military conflict in the Middle East that would eventually bankrupt this country. In 2004, Bin Laden delivered the message that

all that we have to do is to send two Mujahedin to the farthest point East to raise a piece of cloth on which is written al-Qa'ida in order to make the generals race there to cause America to suffer human economic and political losses without their achieving for it anything of note other than some benefits to their private companies. This is in addition to our having experience in using guerrilla warfare and the war of attrition to fight tyrannical superpowers as we alongside the Mujahedin bled Russia for 10 years until it went bankrupt and was forced to withdraw in defeat. So we are continuing this policy in bleeding America to the point of bankruptcy.¹³⁵

Bin Laden's motivation for waging this style of war was because he viewed his territory as being under occupation and the strategy was designed to make the continued deployment of U.S. troops unsustainable. In his videotaped messages, Bin Laden states, "we fight you because we are free men who don't sleep under oppression. We want to restore freedom to our Nation and just as you lay waste to our Nation, so shall we lay waste to yours."¹³⁶ Bin Laden's message showed no interest in invading the United States or eradicating the entire American public.

This freedom fighter warfare strategy is problematic for a conventional military because of the imbalance between the extreme expense of maintaining a remotely deployed modern military force with the minimal expense of conducting guerrilla operations with a small number of operatives and homemade explosives.

¹³⁵ Osama Bin Laden, "Transcript: Translation of Bin Laden's Videotaped Message," *The Washington Post*, November 1, 2004, <http://www.washingtonpost.com/wp-dyn/articles/A16990-2004Nov1.html>.

¹³⁶ Bin Laden, "Transcript: Translation of Bin Laden's Videotaped Message."

H. HOMELAND SECURITY ENTERPRISE VERSUS HOMEGROWN VIOLENT EXTREMISTS

The same imbalances in the costs of waging warfare exist between the thousands of entities in the law enforcement arm of the homeland security enterprise and the homegrown violent extremists who self-radicalize to jihad against domestic targets.

In 2010, Al Qaeda transitioned to a “death by a thousand cuts” strategy, which focused on a high volume of low cost attacks. One example is the plot to use bombs in printer cartridges to destroy planes. This plot had an estimated cost of \$4,200¹³⁷ but would have done hundreds of millions of dollars in damage to the aviation industry by destroying two Boeing 747 aircraft valued at more than \$200 million each,¹³⁸ and causing subsequent groundings of other flights.¹³⁹ Similar to the problems with the military occupation of Iraq and Afghanistan, the cost of maintaining thousands of intelligence analysts and law enforcement officers dedicated to counter-terrorists is unsustainably expensive, while the cost of conducting small-scale terrorist operations is a reasonable expense for Al Qaeda.

Both Al Qaeda’s *Inspire* magazine and the Islamic State’s *Dabiq* offer similar guidance to future jihadists to conduct small attack close to home, such as the message in *Dabiq* No. 6 of “the Muslims will continue to defy the kāfir war machine, flanking the crusaders on their own streets and bringing the war back to their own soil.”¹⁴⁰

I. TERRORIST’S TARGET SELECTION—MAXIMUM EXPOSURE NOT CRITICAL FUNCTIONS

The use of fear as a tactic makes the target selection for a terrorist attack even more complicated to determine. “The potential for misplaced threat-related priorities may

¹³⁷ Matthew Cole, “Al Qaeda Promises U.S. Death by a ‘Thousand Cuts’” *ABC News*, November 21, 2010, <http://abcnews.go.com/Blotter/al-qaeda-promises-us-death-thousand-cuts/story?id=12204726>.

¹³⁸ “Boeing 747-400 Freighter Commercial Cargo Jet,” <http://planes.axleageeks.com/1/279/Boeing-747-400-Freighter>.

¹³⁹ Saad Abedine, “Yemen-based Al Qaeda Group Claims Responsibility for Parcel Bomb Plot,” *CNN*, November 5, 2010, <http://www.cnn.com/2010/WORLD/meast/11/05/yemen.security.concern/>.

¹⁴⁰ “ISIS Releases Issue 6 of Dabiq Magazine,” December 30, 2014, <http://www.clarionproject.org/news/islamic-state-isis-isil-propaganda-magazine-dabiq#>.

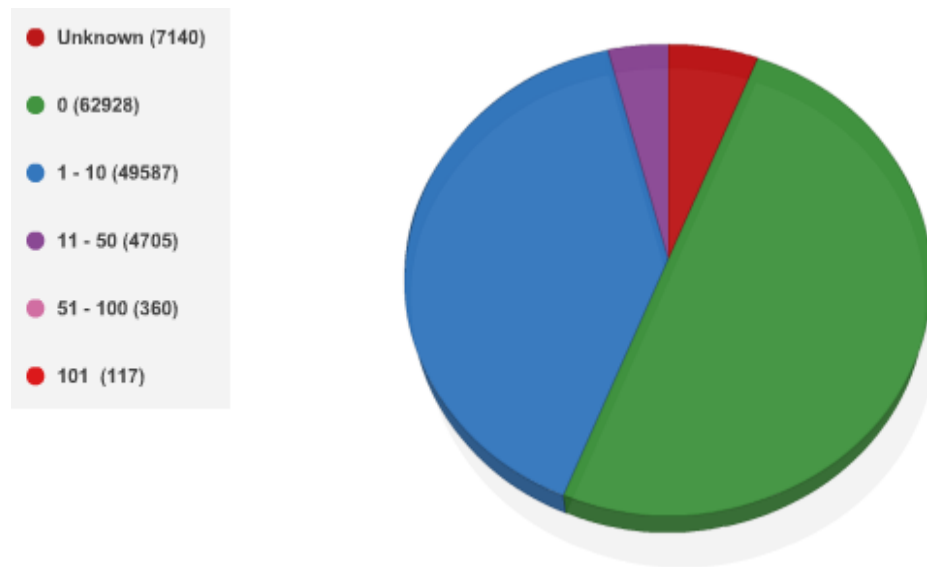
represent a particularly daunting challenge for the United States, which can anticipate a vast array of possible terrorist targets and methods, but relatively to many areas of conflict, it has had little historical experience with terrorist attacks.”¹⁴¹

Without a framework of past experience with terrorism, DHS likely used conventional military strategies to identify domestic CI. One of these sources was likely Sun Tzu’s war strategy, which centered on defeating the enemy with least amount of effort possible. This same strategy has been utilized by the United States in the air bombing campaigns against Iraq. Using Warden’s theory of concentric rings, the highest value targets (the leadership and most CI) are targeted to cripple the remainder of the country. Precise attacks to the strategic core leave the population mostly unharmed.

Terrorism is not about conquering the enemy or using strategic strikes. Since the objectives of a terrorist group are different from an army, CI facilities have lower value and are less likely to be targeted. The intent of the terrorist is to send a message and gain maximum exposure but not necessary cripple the functions of the target. Of the 125,087 incidents in the Global Terrorism Database, more than 74,000 had no injuries and 90% had less than 10 injuries from the attack (Figure 15). Nearly 63,000 also had no fatalities and more than 90% of incidents also had less than 10 fatalities (Figure 15). This small number of injuries and deaths occurred even though 59,982 of the incidents were bombings/explosions targeting primarily private citizens, businesses, military, and government. As shown in Figure 17, less than .5% of the attacks were against telecommunications systems, which are a critical component of infrastructure systems and would be a high value strategic target.

¹⁴¹ Bongar, *Psychology of Terrorism*, 118.

Figure 15. Fatalities from Terrorist Attacks



From “Global Terrorism Database, Search Results: 141966 Incidents,” accessed July 22, 2015, <http://www.start.umd.edu/gtd/>.

The 1995 Aum Shinrikyo attack on the Tokyo Subway using ricin is an example of a terrorist attack that occurred at a critical transportation facility but the intent of the attack was not to cripple the transportation system. The doomsday cult held a belief that the Japanese government was corrupt and responsible for a pending apocalypse, so a shocking attack would cause the people of Japan to prescribe to the Aum Shinrikyo beliefs. Regardless of the reason, this attack was destructive and deadly, but it was not an attack on an infrastructure system; it was an attack on a mass gathering of people inside a vulnerable area.¹⁴²

In Osama Bin Laden’s video tape released taking credit for the 9/11 attack, he said, “the Twin Towers were legitimate targets, they were supporting U.S. economic power. These events were great by all measurement. What was destroyed were not only the towers, but the towers of morale in that country.”¹⁴³ Bin Laden’s statement makes it clear that the attack was not intended to destroy the American economy or collapse the

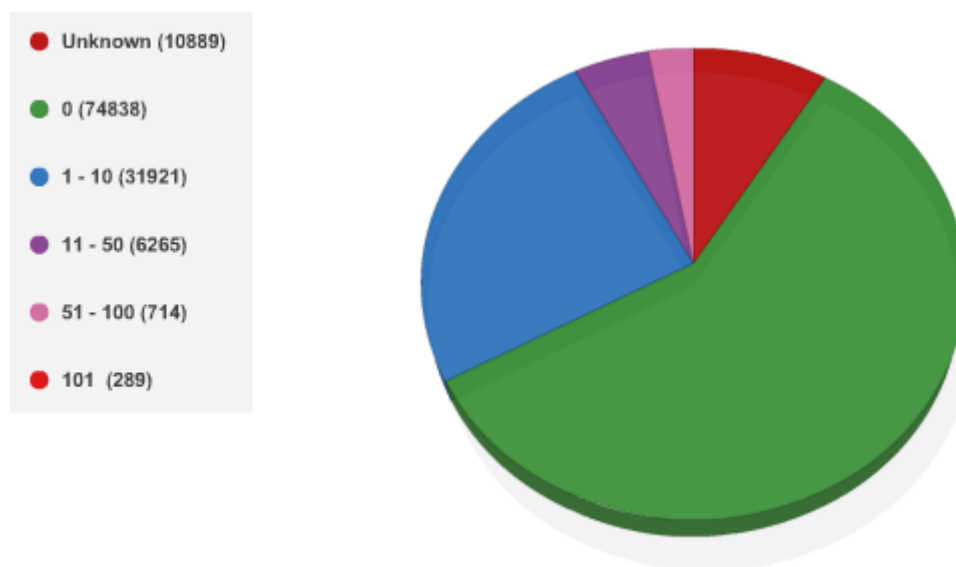
¹⁴² Nicholas Kristof, “A Guru’s Journey—A Special Report; The Seer among the Blind: Japanese Sect Leader’s Rise,” *The New York Times*, March 25, 1995, <http://www.nytimes.com/1995/03/26/world/guru-s-journey-special-report-seer-among-blind-japanese-sect-leader-s-rise.html>.

¹⁴³ David Bamber, “Bin Laden: Yes, I Did It,” *The Telegraph*, November 11, 2001, <http://www.telegraph.co.uk/news/worldnews/asia/afghanistan/1362113/Bin-Laden-Yes-I-did-it.html>.

infrastructure of New York City; the purpose of the attack was to scare and damage the morale of the American people. Like the Irish Republic Army (IRA), and Aum Shinrikyo, the attack was a message, not a targeted strike on CI systems.

Another terrorist group focused on the message of the attack rather than the death and destruction caused by it was the IRA. It was a standard practice of the IRA to call in and report bombings prior to the explosion because the intent of attack was not to harm civilians.¹⁴⁴ As demonstrated in Figure 16, in 74,838 of 125,087 attacks (59.8%), no injuries occurred. Mass injuries harming more than 100 people occurred less than .08% of the time. In the majority of cases, the goal of a terrorist attack has been to send a message rather than cause widespread harm.

Figure 16. Injuries from Terrorist Attacks



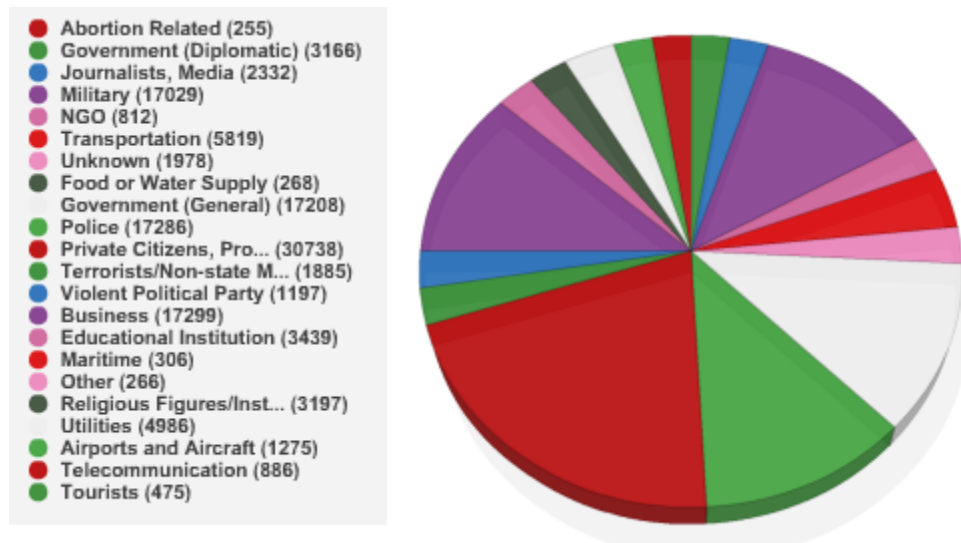
From "Global Terrorism Database, Search Results: 141966 Incidents," accessed July 22, 2015, <http://www.start.umd.edu/gtd/>.

When considering the facilities at risk for a terrorist attack, the CI protection policies do not align to most frequent targets for terrorist groups around the world.

¹⁴⁴ David Sharrock, "IRA Is Not So Ruthless and Always Gives Bomb Warnings," *The Telegraph*, September 19, 2001, <http://www.telegraph.co.uk/news/uknews/1340995/IRA-is-not-so-ruthless-and-always-gives-bomb-warnings.html>.

Shown in Figure 17, the most common targets are private citizens, police, military, and government (general and diplomatic), accounting for 70% of all attacks. Facilities providing purely infrastructure functions, such as telecommunications and utilities, were targeted in 4.4% of attacks.

Figure 17. Terrorist Attack Targets by Type



From “Global Terrorism Database, Search Results: 141966 Incidents,” accessed July 22, 2015, <http://www.start.umd.edu/gtd/>.

J. TERRORIST’S MOTIVATION—ATTENTION AND REWARD

Terrorists killing innocent people does not seem like rational actions to most people in the Western world. Conventional thinking about terrorist tactics and targets would suggest that they want to inflict the most damage on as many people as possible. For this reason, standard practices for protecting CI include building fences, installing traffic bollards, monitoring security cameras, and screening visitors at locations, such as government buildings, commercial offices, stadium, hotels, casinos, sports arenas, museums, and so on.

The motivation for terrorist attacks is also distinctly different from a targeted military strike designed to cripple the infrastructure systems of the enemy. The attack is not about destroying the function of the physical system; it is about sending a message to society. The functions of a “terrorist attack can include:

- showing that the authorities are weak and vulnerable to attacks
- proving that the authorities are unable to control events
- lowering allegiances to the authority institutions
- creating a sense of instability and lawlessness in society
- creating a sense of helplessness among the population
- giving the impression of terrorist organizations as being very powerful
- giving the impression that there will be no end to terrorist attacks until a final victory”¹⁴⁵

These functions of a terrorist attack are not exclusive to Islamic extremists. The same fundamental goals motivated groups like the IRA, Aum Shinrikyo in the Tokyo Subway Ricin Attack, and lone-wolf attacks, such as the Oklahoma City Bombing.

The current CI protection policies that aim to prevent all types of attacks are in many ways similar to the difficulty DHS has with identifying individuals as terrorists.¹⁴⁶ The focus on protecting CI has been identifying all possible targets, building better barriers, installing more security and surveillance systems, and gathering large amounts of real time intelligence. In the same manner that stopping every potential terrorist the moment before they strike is unrealistic, it is also impossible to protect every potential target from every possible type of attack. CI protection should focus on determining the most likely targets and realistic forms of attack that would align with the goals of the terrorists groups. In most cases, the likely targets are not CI facilities.

K. DIFFERENCE BETWEEN CRITICAL AND TARGETABLE FACILITIES

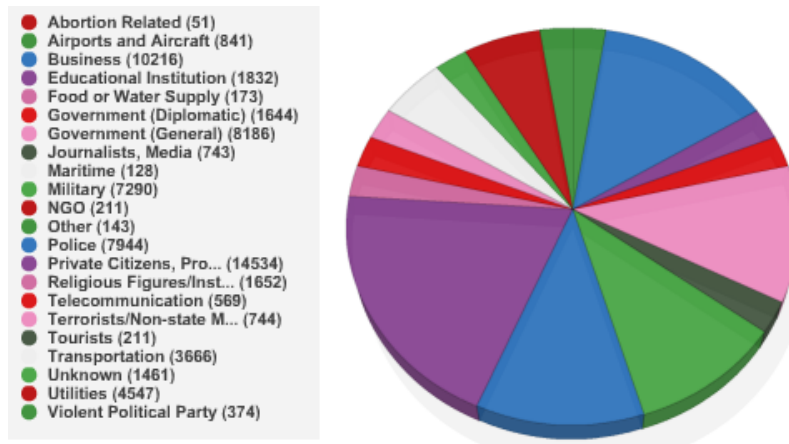
A potential point of confusion in the CI protection mission is the difference between facilities that are part of a CI system and facilities that are attractive targets for terrorism. While a water treatment plant might be a CI facility, its remote location, inaccessibility to the general public, and lack of people at the site, might not make it an

¹⁴⁵ Fathali M. Moghaddam, *From the Terrorists' Point of View What They Experience and Why They Come to Destroy* (Westport, CT: Praeger Security International, 2006), 85.

¹⁴⁶ Johnson, “Remarks By Secretary Jeh Charles Johnson On “The New Realities of Homeland Security” As Part of the Landon Lecture Series on Public Issues—As Prepared For Delivery.”

attractive target for a terrorist. Inversely, an outdoor concert might not serve any infrastructure function but due to the large crowds and open access to the area, it could be an attractive terrorist target. By looking at the types of facilities attacked in the Global Terrorism Database (Figure 18), a difference can be seen between a “targetable” facility and a “critical infrastructure” facility.

Figure 18. Explosive Attacks by Target Type in 62,921 Incidents



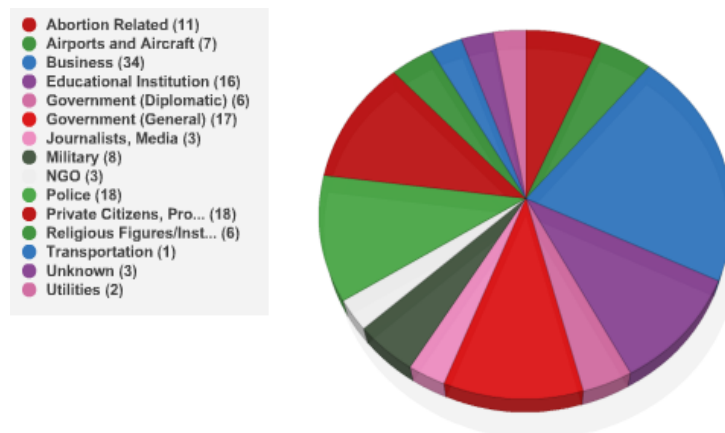
From “Global Terrorism Database, Search Results: 141966 Incidents,” accessed July 22, 2015, <http://www.start.umd.edu/gtd/>.

Looking more specifically at domestic terrorist attacks that have caused 1–10 fatalities or injuries (Figure 19), the Global Terrorism Database includes 149 incidents from 1973 to 2014. The two attacks targeting utilities include the 2012 attempted bombing of a gas pipeline by a sovereign citizen in Plano City, Texas,¹⁴⁷ and the 1976 utility targeted by the New World Liberation Front.¹⁴⁸ The majority of attacks target government, police, private citizens, educational institutions, and businesses. Infrastructure systems including airports, transportation, and utilities are seldom the target.

¹⁴⁷ “Global Terrorism Database, Search Results: 141966 Incidents,” 2015, <http://www.start.umd.edu/gtd/>.

¹⁴⁸ Ibid.

Figure 19. Domestic Attacks Causing 1–10 Fatalities/Injuries



From “Global Terrorism Database, Search Results: 141966 Incidents,” accessed July 22, 2015, <http://www.start.umd.edu/gtd/>.

Since 1970, seven terrorist attacks have occurred in the United States that have killed or injured more than 101 people, as shown in Table 2. These incidents include the 2013 Boston, MA Marathon Bombing, the 9/11 attack at the Pentagon in Arlington, VA, the 9/11 attack at the WTC in New York, NY, the 9/11 plane crash in Shanksville, PA, the 1996 Olympic bombing in Atlanta, GA, the Oklahoma City federal building bombing in 1995, and the 1984 biological (salmonella) attack on The Dalles, Oregon.¹⁴⁹ The target of each bombing was selected to send a specific message from the group responsible for the attack. In each case, the attack did not cause a significant disruption to CI or the functions of the facility attacked, the surround facilities, or government (local, state, or federal).

¹⁴⁹ “Global Terrorism Database, Search Results: 141966 Incidents.”

Table 2. Terrorist Attacks Causing More than 101 Deaths or Injuries in the United States

Attack	Purpose/Intent	Consequence	Disruption to CI	Success?
Boston Marathon Bombing	Establishment of Islamic Caliphate; acceptance in radical Islamist communities; wage war against the United States ¹⁵⁰	Two fatalities, 132 injuries, marathon stopped, minor damage to surrounding buildings	Localized closures at site of explosion (7–10 days), city-wide closures due to law enforcement operations while searching for suspects	Partial—Attack did not harm U.S. military or overseas military operations; Tsarvaev brothers gained acceptance in radical communities
9/11 Attack—Pentagon	Remove U.S. military forces from countries in the Middle East by striking domestic U.S. target with a high profile attack	189 fatalities, 106 injuries, significant damage to a portion of the Pentagon	U.S. Military command functions and U.S. government functions had minimal disruptions to critical operations	No—other than killing/injuring people at the site of the attack, the goals were not accomplished
9/11 Attack—World Trade Center	Remove U.S. military forces from countries in the Middle East by striking domestic U.S. target with a high profile attack; cause widespread fear in public and erode support for government	2,996 fatalities, +6,000 injuries, total destruction of multiple buildings	Localized disruptions to infrastructure functions at the site of the attack and immediate surround areas; regional infrastructure functions experienced minimal disruption	No—other than killing/injuring people at the site of the attack, the goals were not accomplished
9/11 Attack—Shanksville, PA	Remove U.S. military forces from countries in the Middle East by striking domestic U.S. target with a high profile attack; final target unknown	40 fatalities (crew and passengers of AA Flight 77)	None	No—plane crashed prior to reaching intended target

¹⁵⁰ National Public Radio, “The Brothers’ Examines Motivation Behind Boston Marathon Bombing,” April 3, 2015, <http://www.npr.org/2015/04/03/397213144/-the-brothers-examines-motivation-behind-boston-marathon-bombing>.

Attack	Purpose/Intent	Consequence	Disruption to CI	Success?
Atlanta Olympic Games Bombing	Force cancellation of Olympic Games to protest the U.S. governments allowance of abortions	1 fatality, 110 injuries	Olympic Games continued with minimal disruptions; no disruptions to infrastructure functions	No—other than killing/injuring people at the site of the attack, the goals were not accomplished
Oklahoma City Bombing (Murrah Federal Building)	Retaliation against the federal government for gun control and Waco, TX Branch Davidian standoff (attack occurred on 2-year anniversary) ¹⁵¹	168 fatalities, 650 injuries, significant damage to targeted building	Localized disruptions at site of attack; local, state, and federal government continued to function; minimal impacts to infrastructure functions	No—attack did not change government policies
The Dalles, Oregon Salmonella Attack	Sicken the local population prior to election to allow Rajneeshee Group candidate to win election ¹⁵²	0 fatalities, 751 injured, no damage to buildings	No disruption to infrastructure or government functions	No

As these seven attacks demonstrate, targeting and injuring a large number of people does not align with attacking a facility that provides essential infrastructure functions to the nation or region. In each case, the disruptions to essential infrastructure services were nonexistent or minimal in even the immediate areas where the attacks occurred.

Why does CI protection policy focus on large-scale attacks to CI facilities when they have not been the target of the largest domestic terrorist attacks, and were rarely the target of the 130,000 terrorist attacks across the world over the last 50 years?

¹⁵¹ History.com, “Oklahoma City Bombing,” A&E Television Networks, accessed July 22, 2015, <http://www.history.com/topics/oklahoma-city-bombing>.

¹⁵² Public Broadcasting Service, “History of Biowarfare,” 2002, http://www.pbs.org/wgbh/nova/bio/terror/hist_nf.html#cult.

L. TARGETABLE LOCATIONS AND EVENTS

Terrorists are interested in attacking locations that are accessible, crowded with people, have minimal security, and will draw the interest of the general public and the media. The six major terrorist attacks on the United States fit these criteria. For example, the Olympic Park in Atlanta, Georgia was accessible to the general public and had no security screenings. On the local scale, the 10 restaurant salad bars targeted in the 1984 salmonella attacks were easily accessible to the terrorist group, frequented by the public, and the consequences were intended to be widespread across the community. The most recent attack at the Boston Marathon targeted an event open to the general public, did not have security screenings, drew large crowds, and would draw media attention at the local, regional, and national levels. The Boston Marathon attack did not directly target transportation or specific infrastructure functions in Boston with the intent of crippling the city's essential functions.

A terrorist interest lies not in the functions that a facility provides, such as a high demand electrical substation responsible for regional power generation, but instead focuses on accessible areas that are attractive targets for attacks. Targetability is the primary motivation of the terrorist over the criticality of the facility.

M. IMPLICATIONS FOR CRITICAL INFRASTRUCTURE PROTECTION MISSION

Preventing terrorism at the individual level requires developing methods to identify individuals as they ascend up the staircase to terrorism and stop them before they reach the highest level where an attack is planned or carried out. This approach is rooted in the cause rather than the consequence, and can be applied to the CI mission, which should evaluate the motivation and value to a terrorist when determining the risks of terrorist attacks on CI facilities. In the same way that it is impossible to stop every individual from carrying out a terrorist attack, it is impossible to protect every facility from every threat. Evaluating if a facility is a viable target, determining how to protect against the most likely form of attack, and then deciding if a reasonable protective

measure exists that would be a more efficient method of protecting, or not protecting, CI facilities.

Colonel Warden's *The Enemy as a System*¹⁵³ addresses infrastructure as the systems that are so important that "even minor damage to essential industries may lead the command element to make concessions."¹⁵⁴ The concessions may come because:

- Damage to organic essentials/essential systems (CI) leads to the collapse of the system.¹⁵⁵
- Damage to organic essentials/essential systems (CI) makes it physically difficult or impossible to maintain a certain policy or to fight.¹⁵⁶
- Damage to organic essentials/essential systems (CI) has internal political or economic repercussions that are too costly to bear."¹⁵⁷

The homeland security definition of CI is very similar to Warden's concept of organic essentials. DHS defines CI as "the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."¹⁵⁸ Warden states that organic essentials cause a collapse of the system, which is the same as saying "debilitating effects." The systems that make it impossible to maintain a fight are the systems "vital to security, national public health, and safety." The organic essentials that cause great political and economic repercussion are the same as those that endanger the "national economic security." The current definition that DHS uses to describe CI closely aligns with Warden's organic essentials to target during strategic warfare.

The 2013 *National Infrastructure Protection Plan* operates under the assumption that "both domestic and international critical infrastructure assets represent potential prime targets for adversaries. Given the deeply rooted nature of these goals and

¹⁵³ Warden, "The Enemy As a System."

¹⁵⁴ Ibid.

¹⁵⁵ Warden, "The Enemy As a System."

¹⁵⁶ Ibid.

¹⁵⁷ Ibid.

¹⁵⁸ "What is Critical Infrastructure?"

motivations, critical infrastructure likely will remain highly attractive targets for state and non-state actors and others with ill intent.”¹⁵⁹ Based on this research, IP efforts are framed under an inaccurate assumption of the terrorist threat to them. CI protection policies should not be the focus on large-scale attacks to facilities when they have not been the target of the largest domestic terrorist attacks and have rarely been the target of the 130,000 terrorist attacks across the world over the last 50 years. Terrorists have not previously targeted infrastructure and are unlikely to change their intentions in the future, which means that the way DHS views protecting infrastructure and preventing terrorism needs to be reformed.

Much of the current IP analysis conducted by DHS focuses on the attributes of individual facilities within separate functional sectors or subsectors of infrastructure. Military warfare strategies hinge on understanding the entire system that allows an enemy to function and then targeting the weaknesses that causes failures across the system. The focus on individual facilities that provide separate functions lacks the network-wide viewpoint necessary to understand criticalities and assign priorities within the entire infrastructure system, which prevents DHS from accomplishing the statutory protection mission.

¹⁵⁹ Department of Homeland Security, *Supplemental Tool: Executing a Critical Infrastructure Risk Management Approach*.

V. DESTRUCTION OF FACILITIES DHS CURRENTLY DEFINES AS CRITICAL INFRASTRUCTURE AND THE UNEXPECTED RESULTS

The WTC, the Las Vegas Strip casinos, and the toxic contamination of the Elk River in West Virginia (resulting in a municipal water system outage) all serve as unique case studies for challenging the designation of these facilities as CI. Each of these facilities would currently be categorized as critical with the 16 infrastructure sectors. The facilities that DHS designates as CI should cause debilitating impacts to the nation if destroyed, but what if the loss of these facilities did not even have a debilitating impact on a local level? The destruction of the original WTC, the destruction of 14 Las Vegas Strip casinos, and the chemical contamination of the sole water source in Charleston, WV, did not result in debilitating local impacts. Inversely, the New York and Las Vegas cases unexpectedly lead to positive economic impacts at the local level.

It should be noted that the loss of human lives can occur with the destruction of critical facilities, but the IP mission is not always focused on reducing human losses. In 2013, 32,719 traffic collision fatalities occurred on roadways¹⁶⁰ that fall under the CI transportation systems sector but it is the mission of DHS to protect the physical transportation infrastructure from terrorist attacks rather than investing resources to prevent thousands of annual deaths from occurring during vehicle accidents on the highways.¹⁶¹ It is within the scope of DHS mission to assess how a bridge could be attacked with explosives by terrorists, but not to assess if installing higher guardrails could prevent a car from accidentally driving off the bridge.

The CF sector is an example of facilities currently deemed to be CI, but the analysis within the following case studies shows that the buildings were not essential to the nation, not single points of failure, and not providing functions upon which other

¹⁶⁰ National Highway Transportation Safety Administration, *Traffic Safety Facts 2013 Data* (Washington, DC: U.S. Department of Transportation, 2015), <http://www-nrd.nhtsa.dot.gov/Pubs/812181.pdf>.

¹⁶¹ "Transportation Systems Sector," March 25, 2013, <http://www.dhs.gov/transportation-systems-sector>.

infrastructure systems were to depend. If the CF sector is found to not be critical, it may be due to redundant and resilient functions within this sector. As the analysis of the Lower Manhattan office market demonstrated, resiliency occurs within the subsectors, and as a result, the impacts from facility losses were not nationally, regionally, or even locally significant. In New York, when office buildings were destroyed by the 9/11 attacks, others were readily available to absorb the demand for office space within the local market.

Refining the methodology for how facilities are categorized as critical, or not critical, can reduce the total number of CI facilities and the overall complexity of evaluating infrastructure. Removing the “critical” designation from facilities that do not cause national devastation or cascading effects to other infrastructure can be beneficial by allowing DHS to refocus resources on fulfilling the department’s statutory mission of protecting essential infrastructure systems.

A. CASE STUDY: HOW THE LOSS OF WORLD TRADE CENTER WAS CRITICAL TO REDEVELOPING LOWER MANHATTAN

The large brokerage houses that once lined Wall Street and its cavernous side streets have spread far and wide in Manhattan, a reflection of how the area south of Chambers Street is no longer the dominant financial services center it once was. With aging buildings that cannot accommodate huge computers, and a declining need for financial companies to be near each other, The Street and its neighborhood are mere reminders of what they once were.

— *New York Times*, 1994¹⁶²

A steady exodus of banks, brokerage houses and insurance companies in recent years has left the capital of capitalism struggling at the very moment the economic system it epitomizes is sweeping the planet.

— *Boston Globe*, 1996¹⁶³

¹⁶² Thomas Lueck, “Wall Street, No Longer Financial Epicenter, Struggles to Cling to Cachet,” *The New York Times*, December 26, 1994, <http://www.nytimes.com/1994/12/27/nyregion/wall-street-no-longer-financial-epicenter-struggles-to-cling-to-cachet.html>.

¹⁶³ Peter Gosselin, “Wall Street Hits the Wall As Financial World Spins, Leading Firms Depart the Nation’s Economic Capital,” *The Boston Globe*, June 28, 1996, <http://www.highbeam.com/doc/1P2-8373110.html>.

I think it is inevitable that Downtown [Lower Manhattan] will reinvent itself once again. The process is already underway, and I am very optimistic about its future.

— David Rockefeller, 2002¹⁶⁴

It's 1 World Trade Center's stunning combination of ultra-modern design and super-sustainable efficiency that makes it a truly towering achievement.

— WTC.com Marketing Material, 2015

Before September 11, 2001, twin landmark towers stood over the New York City skyline (Figure 20) but many of today's amenities that make Lower Manhattan one of the most valuable real estate markets in the world did not. No Fulton Street Transit Center existed to organize a jumble of train lines and buses. A walkable park hosting more than 500 free concerts and waterfront condominiums stretching along the Hudson River also did not exist. The Downtown Connection bus line did not bring 800,000 annual riders to the area. Thirty billion dollars in combined public and private investment was not available to transform the aging WTC into gleaming Class-A Leadership in Energy and Environmental Design (LEED) Platinum¹⁶⁵ property. Visitors now stay in nearly 8,000 hotel rooms, which is triple the number that existed before 2001.¹⁶⁶

The 9/11 attacks were the largest loss of life in American history from terrorism but out of the rubble, the economic landscape of Lower Manhattan transformed in a manner that would never have been possible without the total loss of WTC.

¹⁶⁴ Alliance for Downtown New York, Inc., *ADNY Annual Report 2014* (New York: Alliance for Downtown New York, Inc., 2014), http://www.downtownny.com/sites/default/files/Annual%20Report_2015_Final_Web2.pdf.

¹⁶⁵ "About: LEED Certification," accessed Retrieved July 23, 2015, <http://www.usgbc.org/leed>.

¹⁶⁶ "ADNY Annual Report 2014."

Figure 20. New York City Skyline in 1995 and 2014



From “ADNY Annual Report 2014,” 2014, http://www.downtownny.com/sites/default/files/Annual%20Report_2015_Final_Web2.pdf.

1. Commercial Real Estate in Manhattan

Manhattan is now one of the largest commercial office markets in the world. According to 2014 tax records, 1,941 commercial office buildings are valued at \$95.6 billion.¹⁶⁷ In 2000, it was assessed at \$42.9 billion¹⁶⁸ (\$58.9 billion adjusted to 2014 inflation¹⁶⁹), which shows the property values have almost doubled in the last 13 years since the 9/11 attacks, as shown in Figure 21.

While the destruction of the WTC caused a major impact to the area, things were not in great shape prior to the attack. The year 1995 was the lowest point in a troubled decade for Lower Manhattan. Nineteen of the 20 largest stock brokerage houses had

¹⁶⁷ Office of Tax Policy, *Annual Report: New York City Property Tax FY 2014* (City of New York: Department of Finance, 2014), http://www1.nyc.gov/assets/finance/downloads/pdf/reports/reports-property-tax/nyc_property_fy14fmvandav.pdf.

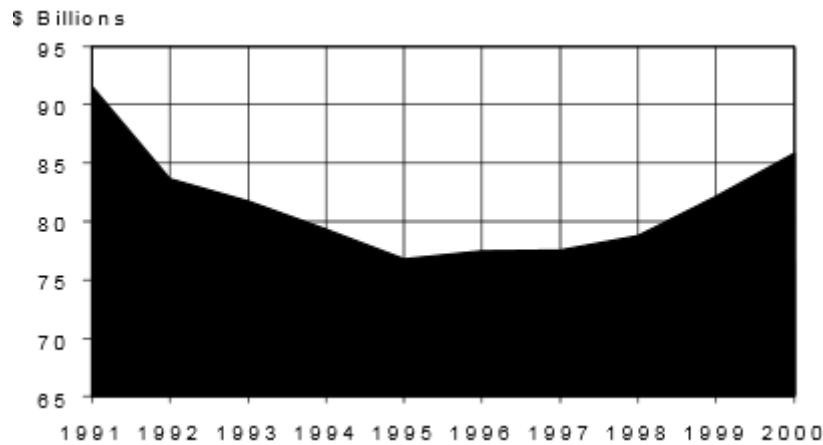
¹⁶⁸ Office of Tax Policy, *Report on New York City Property Tax FY 2000* (City of New York: Department of Finance, 2000), <http://www1.nyc.gov/assets/finance/downloads/pdf/99pdf/rptsum00.pdf>.

¹⁶⁹ “U.S. Inflation Calculator,” accessed July 23, 2015, <http://www.usinflationcalculator.com/>.

closed, 18 of the 20 largest advertising firms had left, and only seven of the original 35 Broadway theaters remained open.

The flight of major brokerage houses and investment banks has left the neighborhood burdened by old office buildings, with nearly a quarter of their space vacant, and with their prospects of luring tenants undermined by small floors, poor ventilation and wiring, and outdated architecture. Now, while they still need larger and more modern buildings than can be found on the blocks around Wall Street, he said the priority of many of the securities companies is to find the best deals they can strike on corporate real estate, with few reservations about moving off the beaten path in Manhattan.¹⁷⁰

Figure 21. Assessed Property Values in Lower Manhattan between New York City Fiscal Year 1991–2000



From Office of Tax Policy, *Report on New York City Property Tax FY 2000* (City of New York: Department of Finance, 2000), <http://www1.nyc.gov/assets/finance/downloads/pdf/99pdf/rptsum00.pdf>.

Tax incentives and large amounts of vacant office space allowed tenants outside the financial industry to move into Lower Manhattan. In 1996, major tenant additions included American Airlines, Pfizer Inc, and Gruner & Jahr USA Publishing. The Mayor's revitalization plan also called for converting office spaces into residential properties. Vacancy rates still remained around 70% and the square footage rate for the American

¹⁷⁰ Lueck, "Wall Street, No Longer Financial Epicenter, Struggles to Cling to Cachet."

Airlines 15-year lease was only \$33 (\$45.3 adjusted to 2014 inflation) per square/foot (the new WTC is currently leasing for \$72/ft).¹⁷¹

At the center of the changing office market, which was transitioning from stockbrokers and advertising to a variety of international businesses, was the WTC towers. The Twin Towers were designed and built during the heyday of big Wall Street brokerage houses and included 7.6 million square feet of space, which were not designed for computers and modern office amenities. In 1995, the WTC had a 25.1% vacancy rate, which meant that nearly 2 million square feet of space were vacant (an entire 40-story high-rise building of empty space).¹⁷² The enormous amount of vacant space at the WTC negatively impacted real estate and rental prices throughout the entire area.

2. Loss of the World Trade Center

In the aftermath of 9/11, without the WTC (original or new) the office space market in Manhattan was well positioned for growth. In 2004, the City of New York Independent Budget Office,

forecasted that office employment would regain the peak it had reached in 2000 by 2010. It appeared that currently vacant space, as well as space expected to come on-line during the 2005–2010 period (i.e., Time Warner Center, 1 Bryant Park, the New York Times building, and the Bloomberg building) would be sufficient capacity to accommodate the new workers even while the trade center buildings remained under construction.¹⁷³

According to the Independent Budget Office,

the destruction of the World Trade Center and damage to surrounding buildings removed roughly 30 percent of the downtown Class-A office inventory. Contrary to expectations, this loss did not result in a spike in rents caused by the precipitous decline in supply. Instead, the spreading

¹⁷¹ Mervyn Rothstein, “The Former Mobil Building, Largely Vacant in the 90’s, Gets a New Tenant, American Airlines,” *The New York Times*, October 29, 1996, <http://www.nytimes.com/1996/10/30/business/former-mobil-building-largely-vacant-90-s-gets-new-tenant-american-airlines.html>.

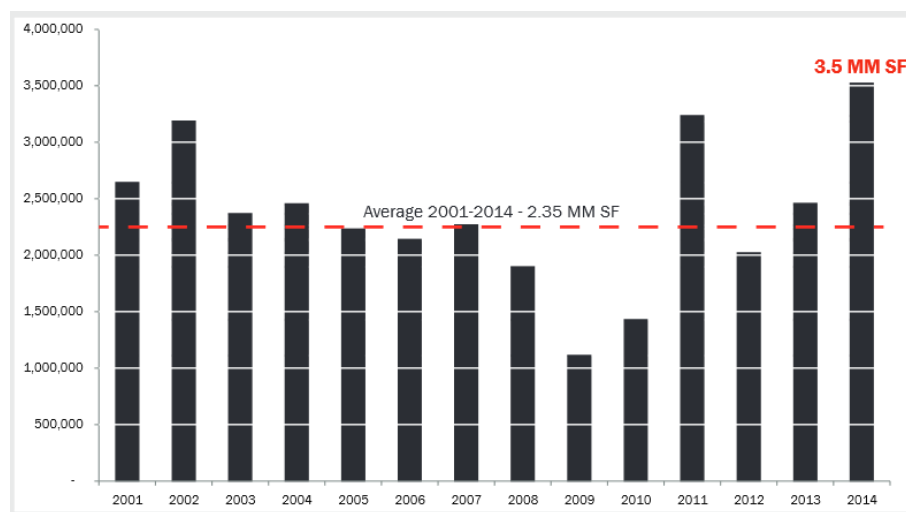
¹⁷² Charles Bagli, “Guardian Insurance’s Plan Adds to Downtown Rebirth,” *The New York Times*, January 8, 1998, <http://www.nytimes.com/1998/01/09/nyregion/guardian-insurance-s-plan-adds-to-downtown-rebirth.html>.

¹⁷³ City of New York Independent Budget Office, *Response to Request to Examine Critical Issues Underlying the Planned Rebuilding at the World Trade Center Site* (City of New York: Independent Budget Office, 2006), <http://www.ibo.nyc.ny.us/iboreports/stringerwtclet.pdf>.

impact of employment losses due to the local recession that had started in the spring of 2001 and accelerated after the attack, combined with the existence of leased but unoccupied ‘shadow space’ in midtown and downtown, enabled the real estate market to absorb most of the displaced tenants with little effect on rents. Instead, downtown vacancies grew and rents fell during 2002 before stabilizing somewhat during 2003 and 2004.¹⁷⁴

As demonstrated by Figure 22, commercial office leasing peaked in 2002 following the loss of the WTC and the need to secure new office spaces. Above-average leasing continued in 2003 and 2004. As the new WTC and other redeveloped Lower Manhattan properties have opened, office-leasing activity peaked in 2013 and 2014.

Figure 22. Lower Manhattan Commercial Leasing Activity 2001–2014



From Alliance for Downtown New York, Inc., *Lower Manhattan Real Estate Market Overview* (New York: Alliance for Downtown, 2014), <http://www.downtownny.com/sites/default/files/Q2%202014%20FINAL%20REPORT.pdf>.

3. Creating New Markets

The criticality of an individual facility, even an enormous commercial facility like the original WTC, is nearly impossible to evaluate because even though it seems to be counterintuitive, the destruction of the old WTC allowed for the creation of a more valuable facility.

¹⁷⁴ City of New York Independent Budget Office, *Response to Request to Examine Critical Issues Underlying the Planned Rebuilding at the World Trade Center Site*.

The original seven building WTC site contained 11.2 million square feet of office space, which accounted for 4% of the total office inventory in Manhattan.¹⁷⁵ If the original WTC were 100% occupied with the hotel maintaining peak average occupancy, the combined site properties would generate a maximum of approximately \$545 million in annual revenue, as demonstrated in Table 3.

Table 3. Original World Trade Center Maximum Leasing Revenue Estimate

Property	Square Footage ¹⁷⁶	Price per Square-Foot	Total (Adjusted to 2014 Inflation)
1 World Trade Center	3.8 million	\$47.00 ¹⁷⁷	\$178,600,000 (\$245,534,550)
2 World Trade Center	3.8 million	\$47.00	\$178,600,000 (\$245,534,550)
3 World Trade Center (Marriott Hotel)	825 hotel rooms	86.7% occupancy X \$280/night X 365 ¹⁷⁸	\$73,101,105 (\$100,497,463)
4 World Trade Center (9-Story Low-rise)	200,000 (estimated ¹⁷⁹)	\$47.00	\$9,400,000 (\$12,922,871)
5 World Trade Center (9-Story Low-rise)	200,000 (estimated)	\$47.00	\$9,400,000 (\$12,922,871)
6 World Trade Center (8-Story Low-rise)	180,000 (estimated)	\$47.00	\$8,460,000 (\$11,630,583)
7 World Trade Center (retail/47 stories)	1.86 million ¹⁸⁰	\$47.00	\$87,420,000 (\$120,182,701)
Total:	14 million ¹⁸¹		\$544,981,105 (\$749,225,591)

¹⁷⁵ “World Trade Center,” July 9, 2015, http://www.newworldencyclopedia.org/entry/World_Trade_Center.

¹⁷⁶ “World Trade Center.”

¹⁷⁷ City of New York Independent Budget Office, *Response to Request to Examine Critical Issues Underlying the Planned Rebuilding at the World Trade Center Site*.

¹⁷⁸ HVS Global Hospitality Services, *2012 Manhattan Hotel Market Overview* (Mineola, NY: HVS Global Hospitality Services, 2012, <http://www.hvs.com/Content/3268.pdf>).

¹⁷⁹ “Key Office Properties,” accessed July 23, 2015, <http://davispartners.com/management/key-office-properties/>.

¹⁸⁰ Federal Emergency Management Agency, *World Trade Center 7 Building Performance Study* (Washington, DC: Department of Homeland Security, 2002), <http://www.fema.gov/media-library/assets/documents/3544>.

¹⁸¹ Jason Bram, James Orr, and Carol Raraport, “Measuring the Effects of the September 11 Attack on New York City,” *FRBNY Economic Policy Review*, November 1, 2002, <http://www.newyorkfed.org/research/epr/02v08n2/0211rapa.pdf>.

To attract tenants from multi-national corporations, and compete with surrounding properties, premium commercial offices are designated as “Class A.” Office space rental prices are grouped in three classes by the Building Owners and Managers Association International (BOMA). The classes include:

- Class A—Most prestigious buildings competing for premier office users with rents above average for the area. Buildings have high quality standard finishes, state of the art systems, exceptional accessibility, and a definite market presence.
- Class B—Buildings competing for a wide range of users with rents in the average range for the area. Building finishes are fair to good for the area. Building finishes are fair to good for the area and systems are adequate, but the building does not compete with Class A at the same price.
- Class C—Buildings competing for tenants requiring functional space at rents below the average for the area.¹⁸²

By today’s standards, the original WTC, which was built in the 1970s, would likely not meet the criteria for a Class A building, and subsequently, would not demand the highest rates and draw the premier tenants paying top dollar. The new WTC is designated “Class A” and if the buildings are 100% leased, the total leasing revenue will exceed \$1 billion annually. See Table 4.

¹⁸² “Building Class Definitions,” accessed July 23, 2015 <http://www.boma.org/research/Pages/building-class-definitions.aspx>.

Table 4. New World Trade Center Maximum Leasing Revenue Estimate

Property	Square Footage	Price per Square-Foot (annual)	Total
1 World Trade Center	3 million (Class A office)	\$72.44 ¹⁸³	\$217,320,000
2 World Trade Center	2.8 million (Class A office)	\$72.44	\$202,832,000
3 World Trade Center	2.5 million (Class A office)	\$72.44	\$181,100,000
4 World Trade Center	2.3 million (Class A office)	\$72.44	\$166,612,000
7 World Trade Center	1.7 million (Class A office)	\$72.44	\$123,148,000
World Trade Center Transportation Hub	350,000 (retail)	\$319.00 ¹⁸⁴	\$111,650,000
	12.65 million		Total: \$1,002,665,000

The new WTC buildings have the potential to generate \$250 million more in annual revenue than the old buildings. This total would likely be much higher because the old Twin Towers would struggle to compete with surrounding premium office spaces or the excess office space across the entire Lower Manhattan office market would collectively drive down properties values. Instead, the new WTC buildings are the cornerstone of the revitalized Lower Manhattan office market.

4. Cost of 9/11 Attack versus Economic Impacts of Redevelopment

A 2002 study by the Federal Reserve Bank of New York Economic and Policy Review estimate the total losses from the 9/11 attacks including earning losses, property damage, and cleanup to be between \$33 and \$36 billion.¹⁸⁵ Of those losses, the physical losses shown in Figure 23 total \$21.6 billion.

¹⁸³ Rey Mashayekhi, "Class A Rents in Midtown Rebound; Midtown South Sees 'Hitch'" *The Real Deal – New York Real Estate News*, May 1, 2015, <http://therealdeal.com/blog/2015/05/01/class-a-rents-in-midtown-rebound-while-midtown-south-sees-hitch/>.

¹⁸⁴ Mashayekhi, "Class A Rents in Midtown Rebound; Midtown South Sees 'Hitch.'"

¹⁸⁵ Bram, Orr, and Raraport, "Measuring the Effects of the September 11 Attack on New York City."

Figure 23. Measuring the Effects of the September 11, 2001 Attack on New York City

Physical capital		
Cleanup and site restoration	\$1.5 billion	Completed June 2002; expenses covered by the Federal Emergency Management Agency (FEMA)
Destroyed buildings in World Trade Center complex	Approximately 14 million square feet, \$6.7 billion to rebuild	Book value of towers at \$3.5 billion; complex privately insured
Damaged buildings in World Trade Center area	Approximately 15 million square feet, \$4.5 billion	Inclusion of damage to Class B and C space raises estimate to 21 million square feet
Contents of buildings in World Trade Center complex	\$5.2 billion	Significant offset from private insurance
Public infrastructure		
Subway	\$850 million	Estimated repair cost; significant offset from private insurance and/or FEMA for repair to all three components of infrastructure
PATH	\$550 million	
Utilities	\$2.3 billion	
Total capital loss	\$21.6 billion	

From Jason Bram, James Orr, and Carol Raraport, "Measuring the Effects of the September 11 Attack on New York City," *FRBNY Economic Policy Review*, November 1, 2002, <http://www.newyorkfed.org/research/epr/02v08n2/0211rapa.pdf>.

While the loss totals appear to be staggering, they are dwarfed by the positive economic impacts of the redevelopment, which were estimated to be \$15.7 billion annually (direct, indirect, and inducted) in a study produced for the Lower Manhattan Development Corporation, as shown in Figure 24.¹⁸⁶

Figure 24. Economic Impact of Redeveloping the World Trade Center Site

Redevelopment of the World Trade Center Site: Summary of Economic Impact: Construction and Operations						
	Direct, Indirect, and Induced Impact of Construction through 2015			Direct, Indirect, and Induced Impact of Operations in 2015		
	Cumulative Output (\$billions) Range	Avg Annual Employment (FTE) Range	Cumulative Tax Revenue (\$millions) Range	Annual Output (\$billions)	Annual Employment (FTE)	Annual Tax Revenue (\$millions)
NYC	14.02 - 15.42	7,760 - 8,530	149 - 184	15.70	76,950	425
NYS	16.38 - 18.02	9,740 - 10,650	261 - 287	16.40	89,820	460
NY-NJ Metro ²	17.62 - 19.38	10,090 - 11,030	411 - 451	16.36	84,820 ³	865

From Appleseed, *Economic Impact of Redeveloping The World Trade Center Site: New York City, New York State, And the New York—New Jersey Area* (New York: Appleseed, 2003), <http://www.renewnyc.org/content/pdfs/Appleseed.pdf>.

¹⁸⁶ Appleseed, *Economic Impact of Redeveloping The World Trade Center Site: New York City, New York State, And the New York—New Jersey Area* (New York: Appleseed, 2003), <http://www.renewnyc.org/content/pdfs/Appleseed.pdf>.

5. Conclusion

The loss of the life at the original WTC was a tragic event but with it, the sudden disappearance of the original WTC buildings caused a significant decrease in total square-footage of available office space, which served to stabilize an oversaturated and declining commercial real estate market in Lower Manhattan. Through public and private investment, the new WTC has been constructed to be more efficient in design that meets the office market demands of premium clientele in Manhattan. The smaller but more luxurious office footprint draws nearly double the price per square-foot and provides more retail, transit, cultural, and public spaces for the general consumer.

The \$21.6 billion estimate of the capital losses¹⁸⁷ (\$16.4 in physical buildings) associated with the 9/11 attack only represent direct losses impacting the WTC itself. CI is defined by the interconnectivity of the systems within each sector and across multiple sectors. Manhattan has an estimated \$804.4 billion office market¹⁸⁸ with 32.8 million square-feet of office space. Compared to the overall office market, the loss of the WTC represented 2% of the total commercial office building value while also being 29% of total office space (in an oversaturated market). In addition to stabilizing the office leasing market, redevelopment has transformed the mid-1990s Lower Manhattan, which did not offer premier real estate, luxury shopping, world class hotels, destination dining, and tourism, into an area that produces cumulative consumer spending of \$5.2 billion annually according to the 2014 Lower Manhattan Real Estate Market Overview produced by the Alliance for Downtown New York.¹⁸⁹

¹⁸⁷ Appleseed, *Economic Impact of Redeveloping The World Trade Center Site: New York City, New York State, And the New York—New Jersey Area*.

¹⁸⁸ New York City Department of Finance, *Tentative Assessment Roll: Fiscal Year 2008* (New York: Department of Finance, 2007), http://www1.nyc.gov/assets/finance/downloads/pdf/07pdf/assessment_report_08.pdf.

¹⁸⁹ Alliance for Downtown New York, Inc., *Lower Manhattan Real Estate Market Overview 2014* (New York: Alliance for Downtown New York, Inc., 2014), <http://www.downtownny.com/sites/default/files/Q2%202014%20FINAL%20REPORT.pdf>.

6. Impact to Critical Infrastructure Definition

The 2006 *Homeland Security Advisory Council—Report on Critical Infrastructure Task Force* reported that the impacts of terrorism and 9/11 extended “well beyond the direct ‘ground zero effects’ and were exacerbated by citizens’ choices based on their altered perception of risk. Ultimately, the ability of CI to full recover from a catastrophe depends on the actions of the consumers.”¹⁹⁰ The exact “ground zero” location of the 9/11 attack has become a tourism destination of itself. The 110,000-square-foot National September 11 Memorial Museum was initially expected to draw 2.5 million visitors per year but exceeded 500,000 visitors during the first two months of operation in May and June 2014.¹⁹¹ The number of hotel rooms in Lower Manhattan near the location of the attacks has tripled since 2001, which demonstrates significant interest as a destination for tourists (Figure 25).

Figure 25. Number of Hotel Rooms in Lower Manhattan



From Alliance for Downtown New York, Inc., *Lower Manhattan Real Estate Market Overview 2014* (New York: Alliance for Downtown New York, Inc., 2014), <http://www.downtownny.com/sites/default/files/Q2%202014%20FINAL%20REPORT.pdf>.

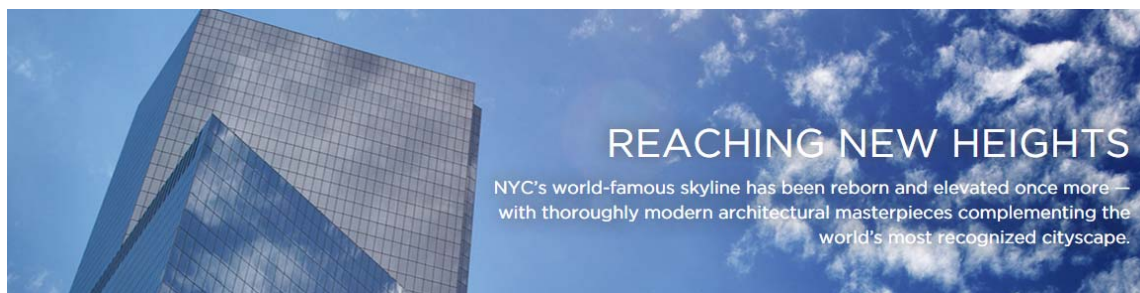
¹⁹⁰ Homeland Security Advisory Council, *Report of the Critical Infrastructure Task Force* (Washington, DC: Department of Homeland Security, 2006), 6, http://www.dhs.gov/xlibrary/assets/HSAC_CITF_Report_v2.pdf.

¹⁹¹ Alliance for Downtown New York, Inc., *Lower Manhattan Real Estate Market Overview 2014*.

The loss of the original WTC is a case that is opposite to the principles of a facility being “critical infrastructure.” Rather than causing debilitating and cascading negative impacts to the nation or surrounding region, the loss of the buildings was a net-positive to the components of the CF sector in Lower Manhattan. It is unlikely a viable plan would have been available to demolish and rebuild the WTC without an unplanned event destroying it. Without the 9/11 attack, the continued existence of the original Twin Towers would have resulted in sustained over-saturation of the Manhattan office market with an excess amount of outdated and undesirable Class B office space. Over the past decade, the office market pressure has continued to grow for LEED Certified and Green Office space, which would have continued to decrease the price per square-foot at the WTC as surrounding buildings drew away Class A customers.¹⁹² The enormous amount of office space within the original Twin Towers would have likely continued to depress the surrounding market and economic growth, and deter capital investment into the area.

The original WTC buildings, and CF in general, should not be considered “critical infrastructure” because commercial markets are too complex with numerous contributing variables for DHS or a group of industry representatives to make assumptions that individual facilities are supremely important. It is very unlikely that anyone would have said the largest building in New York City was not critical, but the destruction of it paved the way for massive redevelopment and economic growth, as seen in Figure 26.

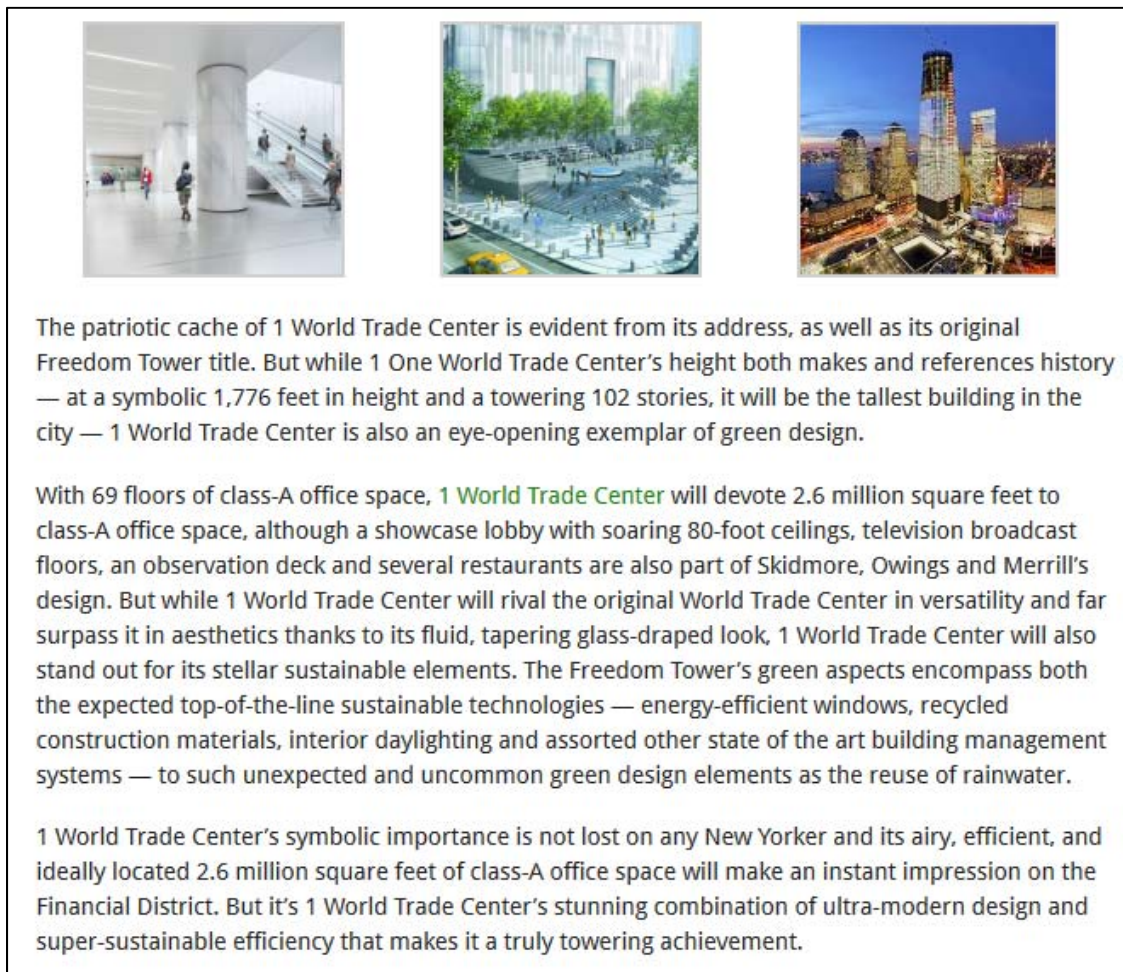
Figure 26. Advertising Materials for the new 1 World Trade Center Building



From “Home: World Trade Center,” accessed July 23, 2015, <https://www.wtc.com/>.

¹⁹² “The Business Case for Green Building,” accessed July 23, 2015, <http://www.usgbc.org/articles/business-case-green-building>.

Figure 27. 1 World Trade Center website



From "One World Trade Center," accessed July 23, 2015, <http://www.greenbuildingsnyc.com/?page=121&cat=36>.

B. CASE STUDY: LAS VEGAS CASINOS AND CRITICAL INFRASTRUCTURE

The *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets* assigned DHS with the responsibility to

develop a uniform methodology for identifying facilities, systems, and functions with national-level criticality to help establish protection priorities; build a comprehensive database to catalog these facilities, systems, and functions; and maintain a comprehensive, up-to-date assessment of vulnerabilities and preparedness across critical sectors.¹⁹³

¹⁹³ Moteff, Copeland, and Fischer, *Critical Infrastructures: What Makes an Infrastructure Critical?*.

Below the national level, DHS's Regional Resiliency Assessment Program evaluates clusters of CI and key resources with a geographic area.

In a regional geographic area, jurisdictions have different interpretations of the types of facilities critical to their jurisdiction, to the larger region and the nation. In Clark County, NV,

the protection of the Nation's infrastructure assets (or "critical infrastructure") from disruption and destruction is a primary function and concern of all levels of government. Clark County, internationally known for the Las Vegas Strip and lavish casino entertainment, is unique in that the structure of the local economy is built primarily on gaming. In the evaluation of critical assets in Las Vegas, Nevada, the most important assets are clearly the casinos and glitter of the Strip.¹⁹⁴

President Policy Direction/PPD-21 defined CI as the "systems and assets, physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health and safety, or any combination of those matters."¹⁹⁵ The *Clark County: Critical Infrastructure and Key Asset* report describes the international and nation significance of Las Vegas and The Strip's casinos as the most critical assets, but are these CF even critical at the local level? See Figure 28.

¹⁹⁴ Urban Environmental Research, LLC, *Clark County: Critical Infrastructure & Key Assets Final* (Clark County, NV: Urban Environmental Research, LLC, 2008, http://www.clarkcountynv.gov/Depts/comprehensive_planning/nuclear_waste/Documents/Studies/CCCriticalInfrastructure0508.pdf).

¹⁹⁵ The White House, *Presidential Policy Directive—Critical Infrastructure Security and Resilience* *Presidential Policy Directive/PPD-21—Critical Infrastructure Security and Resilience*.

Figure 28. Image of the “Fabled” Riviera Casino That Closed on May 4, 2015



From Brandon Griggs, “Fabled Las Vegas Casino Closes after 60 Years,” *CNN*, May 5 2015, <http://www.cnn.com/2015/05/05/travel/riviera-hotel-casino-vegas-closes-feat/>.

1. What Gaming Facilities Subsector Members Expect from DHS

The *National Infrastructure Protection Plan: Commercial Facilities Sector—Annex 2: Gaming Facilities Subsector* describes the facilities in the sector as soft targets vulnerable to the public’s fear and perceptions of security. To protect casinos from potential terrorist attacks, the costs of making physical changes are significant and a need exists for tax incentives to reduce the economic burden on owners for making improvements. The goal of the subsector is to “implement security measures that are efficient, cost-effective, and as unobtrusive as possible.”¹⁹⁶ Across the gaming subsector, facilities have “expressed concerns over sharing assessment information with the Federal

¹⁹⁶ Department of Homeland Security, *Commercial Facilities Sector-Specific Plan an Annex to the National Infrastructure Protection Plan 2010*, 81.

Government for any initiative that makes formal decisions on the prioritization of assets (e.g., concluding that one asset is more ‘at risk’ than another).”¹⁹⁷

The gaming subsector cites \$5.6 billion in direct gaming tax revenue¹⁹⁸ as the justification for federal resources and protection as CI facilities, but the requests of the subsector council include tax incentives, which would reduce this revenue. To distribute resources across 445 facilities effectively, DHS must make a determination of risk, priority, and criticality but the gaming subsector also does not support any effort to document one facility as more important than others.

2. Las Vegas Casinos

In planning for protection of a CI facility, such as a Las Vegas casino, protective measures would address the use of explosives by terrorists to damage or destroy the building. Since the economic depression in 2006, explosives have destroyed many of The Strip’s “critical” casinos but these explosives were planned detonations to implode vacant buildings intentionally. Since 2006, the Castaway, Boardwalk, Bourbon Street, Stardust, New Frontier, and Klondike casinos have all been imploded. During the same time period, the Lady Luck, Sahara, Western, O’Shea’s, Gold Spike, and Riviera casinos have all closed.¹⁹⁹ The implosion of six casinos and the closure of six others over the last decade means that 12 of Las Vegas’ 87 casinos (currently 75 are open), or 14%, of these CI facilities have been lost.²⁰⁰ The loss of a critical facility should result in debilitating impacts to the nation, so how has the loss of 12 critical facilities impacted the local area in Las Vegas?

From 2005 to 2013, the population of Las Vegas has increased from 544,608 to 603,448 (Figure 29). Real per capital income increased slightly from 2005–2007 before dipping to 15% lower than pre-casino closures at \$25,918 in 2013 (Figure 30).

¹⁹⁷ Department of Homeland Security, *Commercial Facilities Sector-Specific Plan an Annex to the National Infrastructure Protection Plan 2010*, 83.

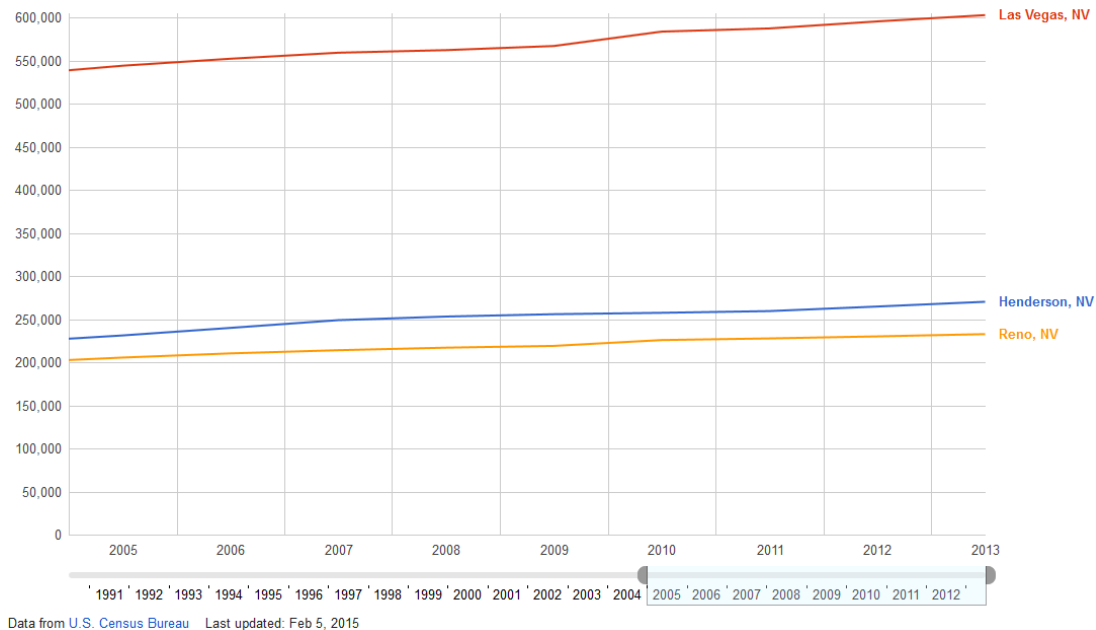
¹⁹⁸ Ibid.

¹⁹⁹ “Yet Another Las Vegas Casino History Timeline,” accessed July 23, 2015 http://www.lvrevealed.com/deathwatch/las_vegas_timeline.html.

²⁰⁰ “Complete List of Las Vegas Casinos,” February 1, 2015, <http://vegasclick.com/vegas/casinos>.

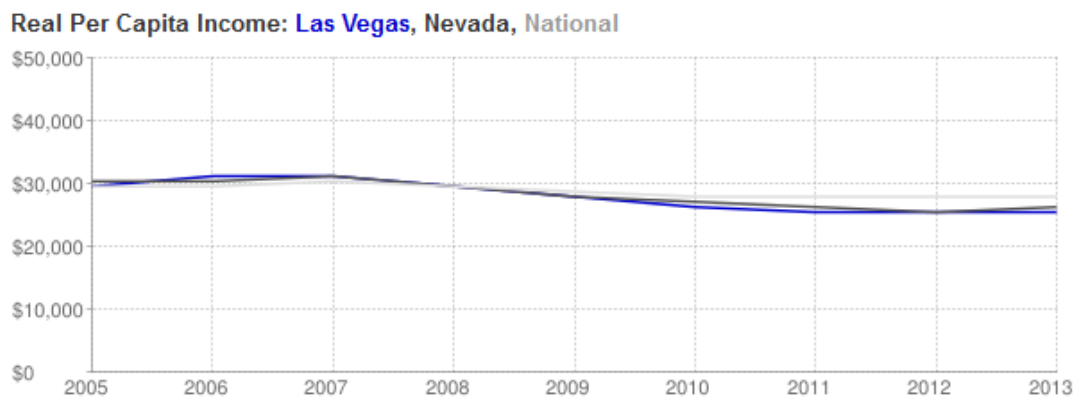
Residential rental rates have remained fairly constant over the same time period (Figure 31).

Figure 29. Population of Las Vegas, NV, by Year



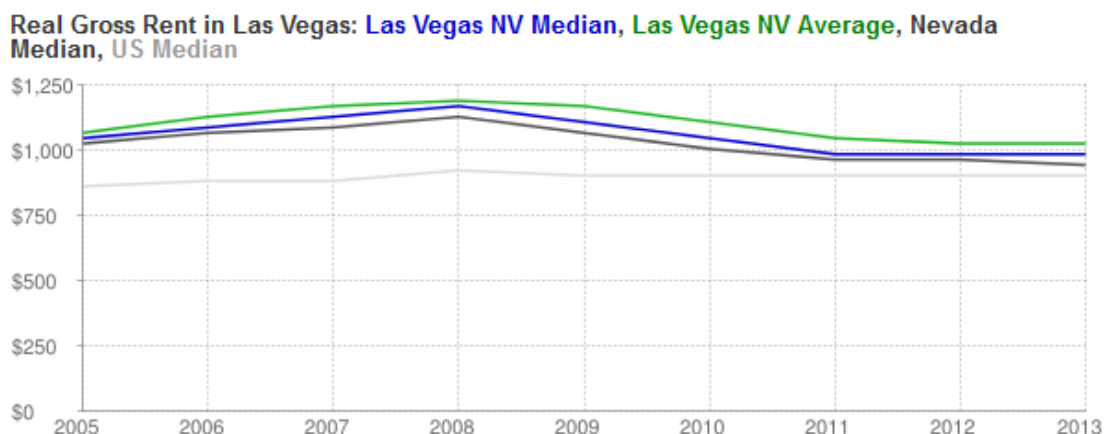
From U.S. Census Bureau, “Public Data from U.S. Census Bureau,” Google.com, February 5, 2015, http://www.google.com/publicdata/explore?ds=kf7tgg1uo9ude_&met_y=population&idim=place:3240000:3260600:3231900&hl=en&dl=en#!ctype=l&strail=false&bcs=d&nselm=h&met_y=population&scale_y=lin&ind_y=false&rdim=country&idim=place:3240000:3260600:3231900&ifdim=country&tstart=1104642000000&tend=1372737600000&hl=en_US&dl=en&ind=false.

Figure 30. Nevada Real Per Capita Income per Year



From “Las Vegas-Paradise Nevada Household Income,” accessed July 23, 2015, <http://www.deptofnumbers.com/income/nevada/las-vegas/>.

Figure 31. Monthly Rental Rates in Las Vegas by Year



From “Las Vegas-Paradise Nevada Rent and Rental Statistics,” accessed July 23, 2015, <http://www.deptofnumbers.com/rent/nevada/las-vegas/>.

In Las Vegas, the casinos are considered to be critical facilities, which would result in debilitating impacts to the local economy if they were destroyed, but as 14% of the casinos were imploded or closed, the population of the city increased while median rental prices and incomes remained fairly constant.

The casinos that have closed permanently or been demolished in Las Vegas had previously been cornerstones of The Strip. The most recent facility to close is the Riviera Hotel and Casino, which was the first high-rise, built in the area in 1955, and included 2,100 hotel rooms. The hotel featured A-list celebrity guests, professional boxing title fights, and performers including Elvis Presley and Louis Armstrong.²⁰¹ While 1,200 employees at the Riviera lost their jobs, more than 950,000 of 1,029,700²⁰² employable people in Las Vegas remain employed maintaining an unemployment rate of 7.2%, which is just over the national average of 5.4%.²⁰³

²⁰¹ Brandon Griggs, “Fabled Las Vegas Casino Closes after 60 Years,” *CNN*, May 5, 2015, <http://www.cnn.com/2015/05/05/travel/riviera-hotel-casino-vegas-closes-feat/>.

²⁰² “Las Vegas-Paradise, NV Economy at a Glance,” July 21, 2015. http://www.bls.gov/eag/eag.nv_lasvegas_msa.htm.

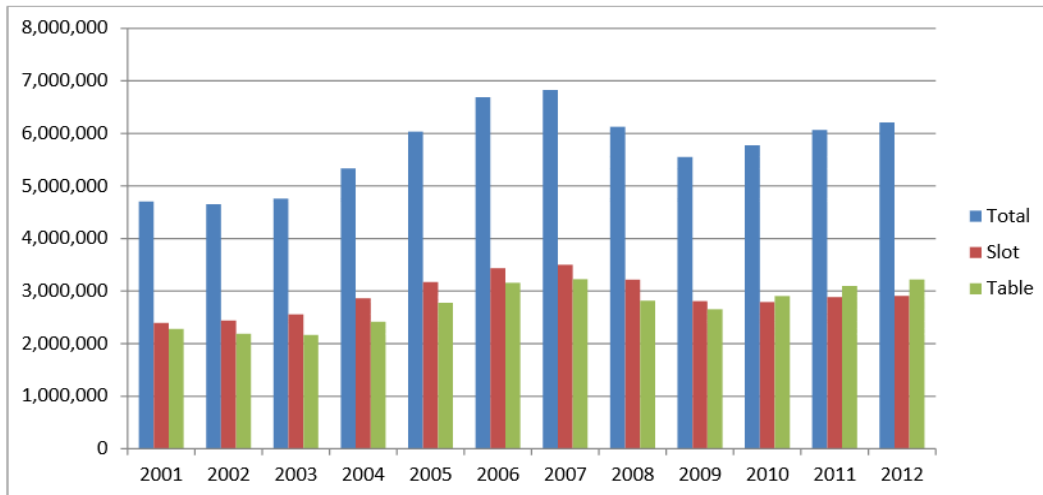
²⁰³ “National Employment Monthly Update,” July 2, 2015, <http://www.ncsl.org/research/labor-and-employment/national-employment-monthly-update.aspx>.

If the loss of “critical infrastructure” casinos in Las Vegas did not result in widespread detrimental impacts to the city, should these facilities be considered to be “critical infrastructure” to Clark County, NV? If the impacts of the closures were negligible at the local level, it is unlikely that these casinos have any regional or national implications to CI.

3. Resiliency within the Las Vegas Casino Industry

While the *Clark County: Critical Infrastructure and Key Asset* report describes The Strip’s casinos as the most critical assets, it is not the individual physical properties that are critical, it is the overall gaming industry that is essential to the city. The individual properties are not critical, as shown by the 12 casinos closed between 2006 and 2015 without causing major disruptions to the tourism industry (Figure 33), hotel occupancy (Figure 33), or gaming revenue (Figure 32). When DHS determines how to spend federal funding for providing protection to CI, not a single casino needs protective measures, and it would be prohibitively expensive to protect every casino against all threats. In a terrorist attack scenario, simultaneously destroying all 80 casinos on the Las Vegas Strip would be the largest terrorist attack in world history, and is very unlikely to occur. The gaming industry in Las Vegas is already “protected” by the resiliency within the network of eight casinos along The Strip. An attack against a single casino, or group of casinos, would not cause the entire gaming industry to crumble because the loss of 12 casinos to closure has not significantly impacted key indicators (visitors, hotel occupancy, and tax revenue). An attack across the entire industry is not realistic. In other words, the protection of the key asset (gaming industry) already exists within the current system without additional assistance from federal funding and resources.

Figure 32. Annual Tax Revenue of Las Vegas Strip Casinos 2001–2012 via University of Las Vegas Center for Gaming Research



From David G. Schwartz, *Major Gaming Jurisdiction: Twelve-Year Comparison* (Las Vegas: Center for Gaming Research, University Libraries, University of Nevada Las Vegas, 2013), http://gaming.unlv.edu/reports/12_year_comp.pdf.

Figure 33. Las Vegas Visitor Statistics from Visitor and Convention Authority

Year	Visitor Volume	Convention		Room Inventory	Occupancy Percentage			LVCVA Room Tax Collections *	En/Deplaned Airline Pass.	Auto Traffic (I-15 at NVCA Border)	Clark County Gaming Revenue *
		Delegates	# Held		Hotel	Motel	Total				
2000	35,849,691	3,853,363	3,722	124,270	92.5%	71.9%	89.1%	130,550,852 r	36,865,866	5,951,009	7,671,252,000 r
2001	35,017,317	5,014,240	20,346 a	126,610	88.9%	63.8%	84.7%	129,053,244	35,179,960 r	5,967,112	7,636,547,000 r
2002	35,071,504	5,105,450	23,031	126,787	88.8%	60.2%	84.0%	127,102,165	35,009,011	37,868 b	7,630,562,000 r
2003	35,540,126	5,657,796	24,463	130,482	89.6%	60.5%	85.0%	138,941,106	36,265,932	38,074	7,830,856,000 r
2004	37,388,781	5,724,864	22,286	131,503	92.0%	68.7%	88.6%	164,821,755	41,441,531 r	38,799	8,711,426,000 r
2005	38,566,717	6,166,194	22,154	133,186	91.8%	72.0%	89.2%	193,136,789	44,267,370 r	39,649	9,717,322,000 r
2006	38,914,889	6,307,961	23,825	132,605	93.2%	65.2%	89.7%	207,289,931	46,304,376 r	40,383	10,630,387,000 r
2007	39,196,761	6,209,253	23,847	132,947	94.0%	64.5%	90.4%	219,713,911	47,729,527 r	39,808	10,868,464,000 r
2008	37,481,552	5,899,725	22,454	140,529	89.8%	57.8%	86.0%	207,117,817	44,074,642 r	37,686	9,796,749,000 r
2009	36,351,469	4,492,275	19,394	148,941	85.3%	50.1%	81.5%	153,150,310	40,469,012 r	39,199	8,838,261,000 r
2010	37,335,436	4,473,134	18,004	148,935	83.5%	52.0%	80.4%	163,809,985	39,757,359	40,213	8,908,574,000 r
2011	38,928,708	4,865,272	19,029	150,161	86.9%	56.0%	83.8%	194,329,584	41,481,204 r	40,344	9,222,677,000 r
2012	39,727,022	4,944,014	21,615	150,481	87.4%	58.0%	84.4%	200,384,250	41,667,596	41,706 r	9,399,845,000 r
2013	39,668,221	5,107,416	22,027	150,593	87.1%	59.8%	84.3%	210,138,974	41,857,059	42,485	9,674,404,000 r
2014	41,126,512	5,169,054	22,103	150,544	89.1%	65.0%	86.8%	232,443,537	42,869,517	42,318	9,554,002,000

From “Historical Las Vegas Visitor Statistics,” February 1, 2015, <http://www.lvcva.com/stats-and-facts/>.

The *Clark County: Critical Infrastructure and Key Asset* report also describes that a terrorist attack would deter visitors from traveling to Las Vegas, which would be extremely detrimental to the hotel and gaming industry. Following the 9/11 attacks in

New York City, annual tourism has increased every calendar year since 2001. In 2013, 54.3 million people visited New York City, which is 16 million more than 2000 (36.2 million).²⁰⁴ The exact site of the terrorist attack has also drawn 19 million visitors to the 9/11 Memorial since it opened in 2011, which suggests that a terrorist attack occurring at a facility is not necessarily a deterrence for future visitors. Furthermore, a memorial for the attack may become a tourist destination in itself.

4. Individual Gaming Facilities Are Not Critical Infrastructure

At the federal level, the gaming facilities subsector uses total gross revenue and tax revenue as the justification for the inclusion of casinos as CI. The DHS gaming subsector also does not identify individual facilities as being more or less critical than other gaming facilities. Choosing not to delineate importance (based on revenue, economic impact, tax base, population, or any other measure) aligns with the concept of the resiliency that has been demonstrated across the Las Vegas Strip casinos. No individual casino in the country has significant impacts at the gaming industry at the local, regional, or national level. A network of hundreds of gaming facilities provides a variety of gambling options even if specific locations are unavailable due to business closure, a terrorist attack, or any other reason. This resiliency within the gaming subsector buffers disruptions and allows for a steady generation of revenue without the need for federal resources to be dedicated to the protection of specific gaming facilities.

C. CASE STUDY: SCARCITY OF FUNCTION AND A SINGLE POINT OF FAILURE FOR CHARLESTON, WV WATER SUPPLY

Clean water is essential to human survival across the world. A mix of public and private utility providers provide water services in the United States, and protection of these critical services falls under the DHS CI water sector. Loss of water services causes both an immediate risk to human health and cascading impacts across other CI sectors dependent on water services.²⁰⁵ Prioritizing the protection of water infrastructure on the

²⁰⁴ “NYC Statistics,” accessed July 23, 2015, <http://www.nycgo.com/articles/nyc-statistics-page>.

²⁰⁵ Department of Homeland Security, *Water Sector-Specific Plan An Annex to the National Infrastructure Protection Plan* (Washington, DC: Department of Homeland Security, 2010), 13, <https://www.dhs.gov/xlibrary/assets/nipp-ssp-water-2010.pdf>.

nationwide level is described in the 2010 *NIPP Water Sector Specific Plan* through the evaluation of “higher-consequence and higher-priority utilities. Four criteria are used to better identify these national level high-consequence assets: (1) population served; (2) amount of chlorine gas stored on site; (3) economic impact; and (4) critical customers served.”²⁰⁶

In January 2014, a toxic chemical spill of 10,000 gallons of 4-methylcyclohexanemethanol contaminated the Elk River one and half miles upstream of the City of Charleston in West Virginia. This spill resulted in the total contamination of water services (drinking, washing, bathing) to 300,000 residents in nine counties.²⁰⁷

Public water utility service was the primary source of water for the majority of the residents in the area:

- 17.6% of residents reported having rainwater and 5.6% reported well water available, which resulted in the majority of residents requiring bottled water because tap water was not available.
- 37% of residents reported using tap water during the “do not use” order, which showed that adequate supplies of bottled water were not available for all water related activities including showering/bathing
- 78.8% of users during restriction showered/bathed with contaminated water.²⁰⁸

The chemical spill into the Elk River is an example of both a scarcity of function and a single point of failure in an infrastructure system. Municipal water service was the primary provider of clean water (an essential-to-life service) for the residents of Charleston and the surrounding counties. Without the municipal water service, a scarcity

²⁰⁶ Department of Homeland Security, *Water Sector-Specific Plan An Annex to the National Infrastructure Protection Plan*, 13.

²⁰⁷ West Virginia Bureau for Public Health (WVBPH) and the Agency for Toxic Substances Disease Registry, *Elk River Chemical Spill Health Effects Findings of Emergency Department Record Review April 2014 Collaborative Investigation by the West Virginia Bureau for Public Health (WVBPH) and the Agency for Toxic Substances Disease Registry (ATSDR)* (West Virginia: Department of Health & Human Resources, 2014), <http://www.dhhr.wv.gov/News/chemical-spill/Documents/ElkRiverMedicalRecordSummary.pdf>

²⁰⁸ Centers for Disease Control and Prevention, *Disaster Response and Recovery Needs of Communities Affected by the Elk River Chemical Spill, West Virginia* (Atlanta, GA: Centers for Disease Control and Prevention, 2014), <http://www.dhhr.wv.gov/News/2014/Documents/WVCASPERReport.pdf>.

of function occurred because other sources were unable to provide adequate supplies of the necessary service to the population. The upstream contamination represented a single point of failure in the water service system because no alternate source was available from which the water treatment facility and water system could draw. The chemical spill into the sole water supply for the majority of citizens caused the entire water service infrastructure to fail.

This failure of the water infrastructure system is an example of a CI system critical to the local jurisdiction. The lack of water services in an isolated area was not regionally or nationally significant to water infrastructure systems. The lack of water to this isolated area was also not debilitating to the region or the nation. This example is useful for studying scarcity of function and single points of failure in a CI system.

Currently, DHS measures the consequences of loss of water services by evaluating the public health effects, economic impacts, psychological impacts, and interdependencies and dependencies with other infrastructure sectors.²⁰⁹ It seems more useful to evaluate the criticality of water systems through the scarcity of the water infrastructure function and the existence of a single point of failure in delivery of the service. At a local and regional level, resiliency in the delivery of essential services exists across infrastructure sectors. In the West Virginia chemical spill, regional and national systems provided bottled and trucked water in an effective manner to meet service demands.

The Charleston outage is useful for evaluating the loss of single sources of essential functions at the national level. The Hoover Dam is the sole provider for providing water serves to 1.3 million citizens.²¹⁰ The Hoover Dam also holds back a 9.2 trillion gallon²¹¹ reservoir that would require million gallons of a toxic chemical to contaminate. In West Virginia, the mining industry positioned 10,000 gallons of a

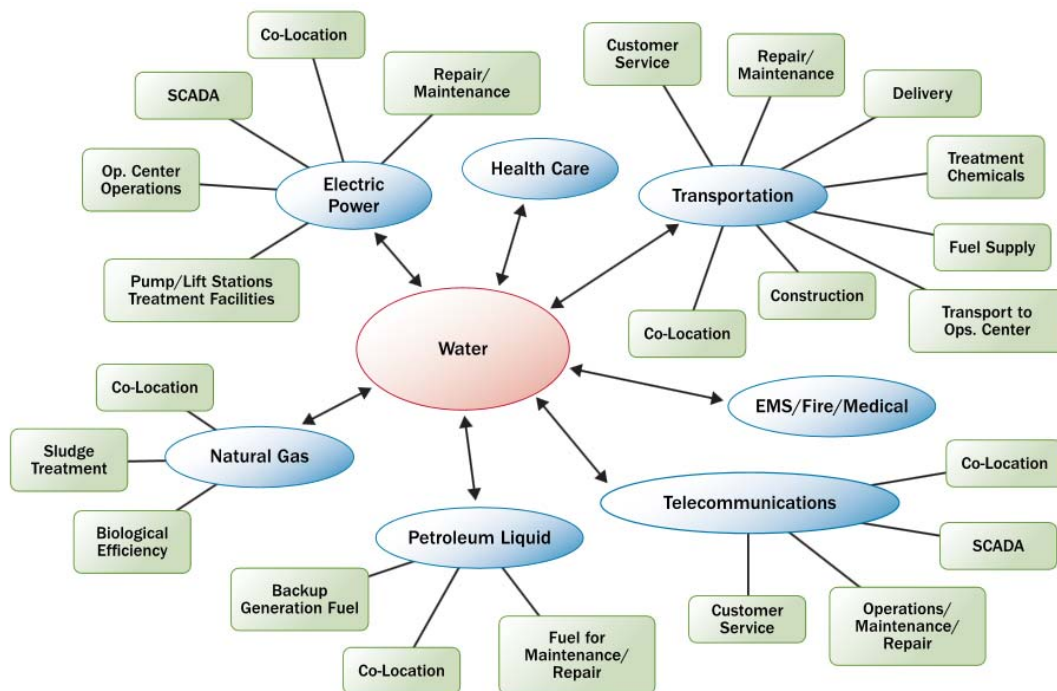
²⁰⁹ Department of Homeland Security, *Water Sector-Specific Plan An Annex to the National Infrastructure Protection Plan*, 25.

²¹⁰ “Hoover Dam—Frequent Asked Questions,” March 12, 2015, <http://www.usbr.gov/lc/hooverdam/faqs/damfaqs.html>.

²¹¹ “Hoover Dam and Powerplant,” September 2013, <http://www.usbr.gov/lc/region/pao/brochures/hoover.html>.

dangerous chemical near a waterway but no million-gallon storage tanks of toxic chemicals are positioned directly around the Hoover Dam. It is also not a viable scenario for a terrorist group, or other enemy, to transport millions of gallons of a toxic chemical to a nationally significant water source. It would take 20,000 tractor-trailer trucks carrying 5,000 gallons of a chemical to amass one million gallons of a contaminant. Even if the Hoover Dam were somehow contaminated with a chemical, it would likely have minimal impact on its ability to generate four billion kilowatts of power,²¹² and the subsequent functions of other infrastructure sectors dependent on it for water.

Figure 34. Interdependencies with Water Sector Infrastructure from National Infrastructure Protection Plan



From Department of Homeland Security, *Water Sector-Specific Plan An Annex to the National Infrastructure Protection Plan* (Washington, DC: Department of Homeland Security, 2010), <https://www.dhs.gov/xlibrary/assets/nipp-ssp-water-2010.pdf>.

On the national level, do sole providers and single points of failure exist in CI systems and services? If they do exist, how large is the scale of the disruption needed to

²¹² “Hoover Dam—Frequent Asked Questions.”

break the system (example: What volume of toxic chemicals would be needed to contaminate the Hetch Hetchy Water System that serves 1.7 million citizens²¹³ in San Francisco, CA? Would an accidental or intentional release of that volume of chemicals be viable? It is likely not a viable scenario?). In the local case of the Charleston spill, water for drinking, cooking, and bathing was impacted but did the contamination have any impact on other infrastructure systems, such as electrical power, telecommunications, transportation, petroleum liquid, or natural gas as shown in Figure 34 from the *National Infrastructure Protection Plan*? A drinking water outage is not necessarily an outage of all water uses across every infrastructure function that uses water as a component of providing its function.

²¹³ “Hetch Hetchy Water System,” accessed July 23, 2015, <http://bawscs.org/water-supply/hetch-hetchy-water-system/>.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. POTENTIAL SOLUTIONS

DHS can simplify the statutory IP mission by removing the designation of “critical” from facilities not essential to the health and safety of the public and the economic security of the nation. Many facilities currently deemed critical are likely not even critical to the region and locality that they serve as shown by the case studies of New York, Las Vegas, and Charleston, WV. To identify facilities more effectively that are CI, DHS should consider a risk-based approach within a more narrow definition of CI modeled after best practices from the United Kingdom. DHS should also reexamine why infrastructure facilities have been designated to be primary targets for terrorism. CI protection policy should not be focused on large-scale attacks to CI facilities when they have not been the target of the largest domestic terrorist attacks and were rarely the target of the 130,000 terrorist attacks across the world over the last 50 years.

DHS is required to manage risks to CI by the *NIPP*, *PPD-21*, and the Homeland Security Act of 2002 but “DHS is not positioned to manage an integrated and coordinated government-wide approach for CI vulnerability assessment activities as called for by the *NIPP*.”²¹⁴ A remedy for this problem is reducing the overall number of facilities across the 16 CI sectors. Removing the low-risk and non-critical facilities can simplify the overall task by reducing the total number of locations, and the subsequent time and resources needed to conduct assessments, plans, sector outreach, working group meeting, and national-level program management. Each of these actions would be easier to accomplish with a smaller number of CI facilities to assess.

While the 2013 *National Infrastructure Protection Plan* provides a supplemental tool for executing a risk management approach, the methodology is too broad because it can apply to “all threats and hazards, including cyber incidents, natural disasters, man-made safety hazards, and active of terrorism, although different information and

²¹⁴ Government Accountability Office, *Critical Infrastructure Protection DHS Action Needed to Enhance Integration and Coordination of Vulnerability Assessment Efforts*, 37.

methodologies may be used to understand each.”²¹⁵ While a national plan should have a specific strategy, the NIPP “goals and objectives are likely to vary across sectors and organizations depending on the risk landscape, operating environment, and composition of a specific industry, resource, or other aspect of critical infrastructure.”²¹⁶ The plan states the importance of measuring effectiveness but the end state and performance metrics are undefined. Adopting a more focused risk-based approach, such as the methods used by the United Kingdom, can assist DHS in evaluating if terrorism is the primary risk to a facility.

A. RECOMMENDATION: FOLLOW BEST PRACTICES FROM ANALYSIS OF THE UNITED KINGDOM’S CRITICAL INFRASTRUCTURE POLICY

Key similarities allow for a comparison of the U.S.’s and the UK’s CI policies. Both countries view the protection of CI as a national security priority because the loss of CI facilities or systems would cause devastating impacts to the safety and health of the public, economy, and the overall well-being of the country.

The UK’s definition of CI is more refined in describing both the core term and definition. Rather than just “critical infrastructure,” the United Kingdom uses the term “national infrastructure” to emphasize the scope of the mission, which is focused on facilities impacting the entire nation. The United Kingdom defines national infrastructure as “facilities, systems, sites and networks necessary for the functioning of the country and the delivery of the essential services upon which daily life in the UK depends.”²¹⁷ The definition makes it clear that national infrastructure is exclusively the systems that the entire country is dependent on for daily life. It can be a best practice adopted by the United States. Both the United States and the United Kingdom understand facilities and systems that provide vital services to the country need to be protected against natural

²¹⁵ Department of Homeland Security, *Supplemental Tool: Executing a Critical Infrastructure Risk Management Approach*.

²¹⁶ Ibid.

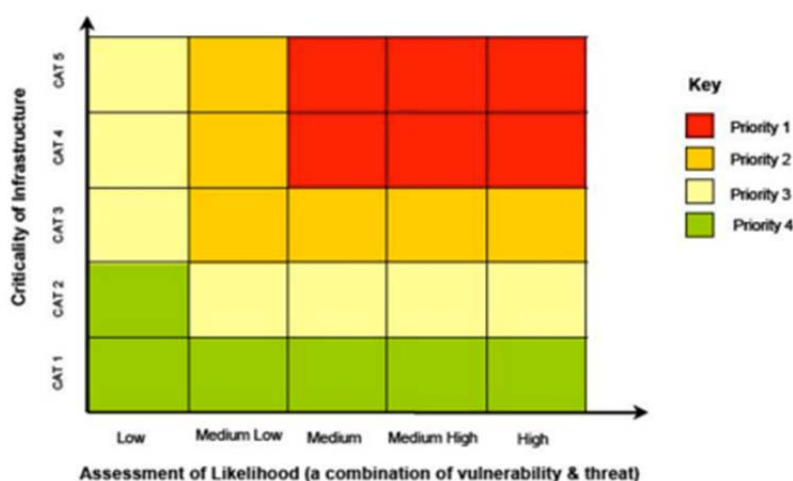
²¹⁷ “About: The National Infrastructure,” accessed July 23, 2015, <http://www.cpni.gov.uk/about/cni/>.

disasters and terrorist attacks. Both countries designate these facilities and systems as “critical infrastructure.”

B. HOW THE UNITED KINGDOM IS PROTECTING INFRASTRUCTURE

Since the resources needed to protect infrastructure assets are limited, and vulnerabilities at every facility are unequal, a way needs to be created to prioritize facilities to guide the protection mission. The United Kingdom uses a risk-based system for prioritizing infrastructure, as shown in Figure 35.

Figure 35. Using a Risk-Based Approach to Prioritize Sector Resilience Planning



From Cabinet Office, *Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards* (United Kingdom: Cabinet Office, 2010), <https://www.gov.uk/government/publications/strategic-framework-and-policy-statement-on-improving-the-resilience-of-critical-infrastructure-to-disruption-from-natural-hazards>.

When assessing risks to CI, the United Kingdom evaluates the likelihood of something happening in the next five years, and the consequences or impacts that people will feel if it does occur.²¹⁸ After determining the risk, the consequence is measured on a

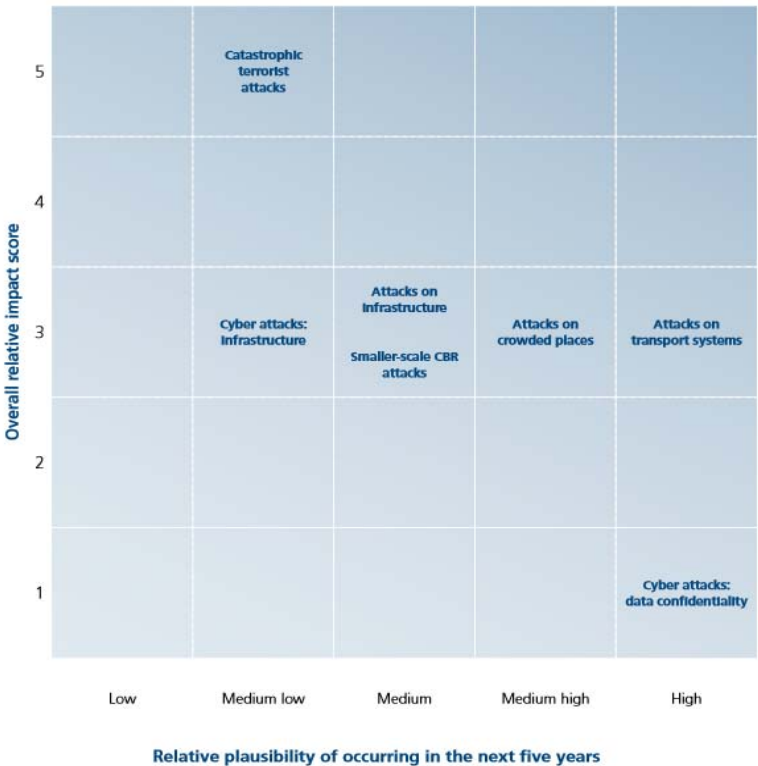
²¹⁸ Cabinet Office, *Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards* (United Kingdom: Cabinet Office, 2010), 2, <https://www.gov.uk/government/publications/strategic-framework-and-policy-statement-on-improving-the-resilience-of-critical-infrastructure-to-disruption-from-natural-hazards>.

0–5 scale based on the number of fatalities, illness/injury caused, social disruptions, economic harm, and psychological impact.²¹⁹ A matrix allows for infrastructure assets to be plotted based on criticality to the nation and the assessment of likelihood from combining vulnerability and existence of a threat. For an infrastructure asset to be considered high priority, both a high level of criticality and a high likelihood of something occurring must be demonstrated.

This risk-based approach is used for both the prioritization of facilities and evaluation of security threats. As Figure 36 depicts, the highest priority attacks would be displayed in the upper right while the lowest priorities would fall in the low left due to low plausibility of occurring and low impact scores. The matrix-based risk assessment allows senior leaders and planners to decide objectively how they want to address risks. A senior leader who is most concerned with high impact/consequence attacks, would be able to look at the matrix and decide, “catastrophic terrorist attacks” are the areas to which resources should be allocated. If a senior leader wants to dedicate resources to the highest likelihood of attack, “attacks on transportation systems” and “cyber-attacks” would be the priority. This type of objective analysis of risk allows a senior official to make informed decisions.

²¹⁹ Cabinet Office, *Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards* (United Kingdom: Cabinet Office, 2010), 4.

Figure 36. Risks of Terrorist and Other Malicious Attacks



From Cabinet Office, Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards (United Kingdom: Cabinet Office, 2010), 10, <https://www.gov.uk/government/publications/strategic-framework-and-policy-statement-on-improving-the-resilience-of-critical-infrastructure-to-disruption-from-natural-hazards>.

Table 5 shows the similarities and differences between the infrastructure sectors designated by the United States compared to the United Kingdom.

Table 5. Comparison of U.S. and U.K. Infrastructure Sectors

U.S. Critical Infrastructure Sectors ²²⁰	U.K. National Infrastructure ²²¹
Chemical*	
Commercial Facilities*	
Communications	Communications
Critical Manufacturing*	
Dams*	
Defense Industrial Base*	
Emergency Services	Emergency Services
Energy	Energy
Financial Services	Financial services
Food and Agriculture	Food
Government Facilities	Government
Health Care and Public Health	Health
Information Technology	
Nuclear Reactors, Materials, and Waste*	
Transportation Systems	Transport
Water and Wastewater Systems	Water

*Privately owned and operated

While the GAO report highlights the issues DHS is having with prioritizing CI protection, the United Kingdom addresses the problem of determining what is critical or non-critical by using a risk-based approach for evaluating facilities within the infrastructure sectors. Not everything within a national infrastructure sector is critical. Within the sectors are certain critical elements of infrastructure, “the loss or compromise of which would have a major detrimental impact on the availability or integrity of essential services, leading to severe economic or social consequences or to loss of life.”²²² These critical assets make up the nation’s critical national infrastructure (CNI) and are referred to individually as “infrastructure assets.” Infrastructure assets may be physical (e.g., sites, installations, pieces of equipment) or logical (e.g., information networks, systems).²²³

²²⁰ “Critical Infrastructure Sectors.”

²²¹ “About: The National Infrastructure.”

²²² “About: The National Infrastructure.”

²²³ Ibid.

C. RECOMMENDATIONS FOR POLICY REVISION

While U.S. CI policies allow for broad inclusiveness of facilities within the sectors, the United Kingdom makes a clear designation that the loss of the infrastructure asset must have a major detrimental impact to the country. The United Kingdom uses a risk-based approach to determine how resources will be allocated and protection of facilities will be prioritized. The United States should adopt a similar risk-based approach that establishes values for prioritization of critical facilities based on criticality, vulnerability, and threat. By using a risk-based matrix to evaluate current CI sectors, the United States could realign the current 16 CI sectors to match the nine used by the United Kingdom. Reducing the total number of infrastructure sectors would simplify the overall protection mission because each sector would have its own dedicated DHS staff, reporting requirements, resource allocation, supporting federal agencies, and performance metrics.

The United States could reduce the number of CI sectors by removing the sectors owned, operated, and protected by the private sector (CF sector, chemical, and critical manufacturing). Individual facilities within these sectors are unlikely to cause catastrophic national impacts if they are destroyed or inoperable. These facilities also do not meet the UK's definition of national infrastructure.

Along the same lines, "information technology" is a nebulous term for designating a sector as critical and is not a term used by the United Kingdom for national infrastructure. The sector is defined as the "virtual and distributed functions produce and provide hardware, software, and information technology systems and services, and—in collaboration with the Communications Sector—the Internet."²²⁴ These systems or components are unlikely to cause catastrophic damages to the entire nation if they are in operable, which makes the designation of CI unnecessary. The systems critical to communication can be addressed under the responsibilities of the communications sector.

²²⁴ "Information Technology Sector," June 12, 2014, <http://www.dhs.gov/information-technology-sector>.

Accordingly, “nuclear reactors” do not need to be a separate CI sector from “energy,” which would also align with the UK national infrastructure designations. The energy produced by a nuclear power plant is critical to the U.S. electric power system. It is unlikely that a nuclear power plant not currently producing power would cause catastrophic consequences if it was attacked or damaged by a natural disaster. The protection of large quantities of nuclear material is likely a separate national security mission that would be carried out by DOD, the Department of Energy, and the Nuclear Regulatory Commission rather than being designated a CI protection mission under the authority of DHS.

Beyond just looking at damage or the loss of infrastructure assets, the term “resilience” is instrumental to UK CI protection. The Cabinet Office defines resilience as the ability to absorb, respond to, and recover from emergencies.²²⁵ When facilities are damaged by a disaster or attack, if the facility provides a critical function, a resilient facility may be able to continue to function or be minimally disrupted.

In the publically available annual *Sector Resilience Plans*, the Cabinet Office provides information about the hazards/threats to each of the nine sectors. The report also provides a summary of the existing level of resilience to address the hazards/threats and actionable recommendations for increasing resilience. For example, in the 2014 plan, the food sector highlights its risk as a “widespread dependency on other essential services, such as fuel.” The resilience of the sector is demonstrated by the ability to “continue to operate at or near to capacity despite the severe winter weather and flooding events experience from 2010 through to early 2014,” and the sector can be strengthened by “government sponsored research looking at the resilience of the food supply chain to port disruption and pinch points created by potential fuel disruptions.”²²⁶ Publishing policies for addressing current risk and conducting future planning to mitigate further risk is a transparent method of addressing shortfalls, while acknowledging the efforts to make CI assets more resilient.

²²⁵ “Emergency Planning,” accessed July 23, 2015, <https://www.gov.uk/government/policies/emergency-planning>.

²²⁶ “A Summary of the 2014 Sector Resilience Plans,” August 1, 2014, <https://www.gov.uk/government/collections/sector-resilience-plans>.

The United Kingdom publishes annual public reports that highlight successes and shortfalls across each of the infrastructure sectors without compromising sensitive information or pointing blame. DHS should adopt this transparent method of informing the public and governmental stakeholders about the status of accomplishing the IP mission. The negative findings of the 2012 GAO report would likely not have occurred if an annual report were published providing a clear picture of the IP mission across each sector.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

Based on this research, very few facilities are critical to the nation. The nationally significant facilities are likely too large or too secure for a terrorist group to destroy, and also not aligned with the targets of previous attacks. On a local and regional level, redundancy and resiliency occur across infrastructure systems that allow affected areas to absorb outages and unaffected areas to provide alternative services. As a backstop, national capabilities can quickly deliver essential services during outages, such as the bottled water supplied to Charleston, WV following the chemical spill. Also, the enormous complexity within the infrastructure systems makes predicting the impacts of outages extremely difficult, as demonstrated by the unanticipated economic gains in Lower Manhattan following the 9/11 attacks. The destruction of supposedly critical facilities has demonstrated that greater resilience does occur across infrastructure systems than DHS generally assumes. Instead of focusing protection efforts on potential losses, greater value may be found in understanding existing resiliency.

A. FINDINGS

This research examined the federal IP policies that have been issued over the past 35 years to determine the origin and evolution of the mission. Within these documents, a consensus can be drawn that the definition of the term “critical infrastructure” is the systems and assets nationally significant and the loss of which would result in debilitating consequences to the safety and security of the United States. The 10 overarching CI policies²²⁷ released over the past 19 years consistently describe CI as being nationally significant, providing vital services, being part of an interconnected system, causing debilitating impacts if destroyed, and providing a service necessary to the health and safety of the general public.

Based on the analysis, infrastructure that lacks national significance, criticality, and interconnectedness to other infrastructure systems does not meet this definition. As a

²²⁷ *Quadrennial Homeland Security Review, NIPP, PPD-21*, Exec. Order No. 13636, *NIPP, National Security Strategy, HSPD-7, USA PATRIOT Act, PDD/NSC-63*, and Exec. Order No. 13010.

result, a discrepancy occurs between the federal policies that define CI and how DHS currently addresses its statutory IP mission to identify, prioritize, and protect the nation's most vital infrastructure.²²⁸

A problem with the current policies is that many of the facilities currently designated as critical do not meet the consensus definition identified in the literature review but are still considered to be "critical infrastructure." This may have stemmed from the early directive for the newly formed DHS to develop a list of all of the critical facilities across the country.²²⁹ This thesis demonstrated challenges DHS has faced from the creation of the NADB, the NCIPP, and the ongoing mandate to develop a centralized list of CI.

Modern military theories provide a potential explanation for the focus of DHS's efforts because the threats from terrorism have likely been evaluated based on the education and experience of senior officials drawing on their experiences with the principles of strategic warfare. Nationally significant infrastructure facilities that can cripple the essential functions of the entire country would be attractive targets for an enemy nation-state to strike with ballistic missile and airpower capabilities during a war. The current terrorist threat comes from homegrown violent extremists and members of terrorist groups who are motivated to inflict mass casualties in the locations that are most visible and easily accessible.²³⁰ An individual terrorist or a small group of terrorists most likely lack the intelligence, organizational coordination, manpower, and resources to conduct a strategic warfare campaign against nationally significant infrastructure targets with the intent of crippling essential-to-life systems across the country. The strategic warfare approach of developing a static list of vulnerable assets does not match the unpredictable and dynamic threat from terrorism. The current IP policies identify the likely targets of a nation-state army and assume them to be the same targets that terrorists would have the intention and capability of attacking.

²²⁸ The White House, *Presidential Policy Directive—Critical Infrastructure Security and Resilience* *Presidential Policy Directive/PPD-21—Critical Infrastructure Security and Resilience*.

²²⁹ United States Congress, *Committee Reports 109th Congress (2005–2006) House Report 109-713—Part 1*.

²³⁰ "Countering Violent Extremism."

The concept of protecting CI could altogether be a wasted effort because when supposedly CI is destroyed, the impacts are often negligible, or in some cases, even results in economic gains. Even when terrorists do successfully strike, the consequences may be more complex than making a blanket assumption that all CI facilities should be protected under all circumstances. Case studies of the WTC and the Las Vegas Strip casinos challenge the general assertion that negative economic consequences always result from the destruction of a “critical” facility. A case study of the 2014 toxic chemical spill into the primary water source serving Charleston, WV provides an example that is contrary to the assumption that the loss of a facility serving as a sole provider of an essential-to-life service results in cascading, debilitating impacts across all infrastructure sectors.

While it was unforeseeable at the time, the Lower Manhattan area most heavily impacted by the 9/11 attacks is more valuable today and better positioned for the future than it was prior to 2001. If terrorists cannot cripple this nation by toppling 100-story commercial high-rise buildings, what kinds of facilities would have a debilitating impact on the entire nation if they were destroyed? Instead of being designated “critical,” the majority of infrastructure facilities are insignificant to the functions of the overall system because the loss of these facilities does not cause widespread disruptions to the nation, region, or even the local area.

B. CONCLUSIONS

The evidence presented within this thesis argued that DHS is not fulfilling the mission of protecting the infrastructure that is critical to the nation by expending resources on misaligned efforts at thousands of insignificant facilities. These problems are rooted in the current scope of the infrastructure mission being too large, but is further complicated because the types of facilities designated as critical may not be the likely targets of terrorists. The few facilities critical to the nation are most likely are too large, too remote, or too secure for a terrorist group to destroy, or to have an interest in targeting.

On a local and regional level, redundancy and resiliency occurs across infrastructure systems that allow affected areas to absorb outages and unaffected areas to provide alternative services. As a backstop, national emergency response capabilities can quickly deliver essential services during outages, such as the bottled water supplied to Charleston, WV following the chemical spill into the water supply. Also, the enormous complexity within infrastructure systems makes predicting the impacts of outages extremely difficult, as demonstrated by the unanticipated economic gains in Lower Manhattan following the 9/11 attacks.

Based on this thesis, DHS should ensure that everything designated as “critical” meets the definition of criticality, that the methodologies used for evaluating infrastructure align to the mission of protecting the nation for terrorism, and that protection efforts account for the existing resiliency within the systems that provide essential-to-life infrastructure across the country.

Many infrastructure facilities are inconsequential if attacked, and if the loss of a facility does not cause the widespread disruptions, it is not CI. DHS should shift from an inclusive CI policy that allows facilities to self-designate and self-assess risks to a policy that assumes facilities are inconsequential to the security and functions of the nation unless proven otherwise.

C. RECOMMENDATIONS

A solution for accomplishing the task of effectively identifying, prioritizing, and protecting CI is refining the criteria for how facilities are determined to be critical. A lower number of critical facilities will reduce the overall scope of the protection mission. To identify facilities CI more effectively, DHS should consider using a risk-based approach within a more narrow definition of the term that can be modeled after best practices from the United Kingdom. The United Kingdom uses the designation of “national infrastructure” to emphasize the scope of the mission, which is focused exclusively on the systems that the entire country is dependent on for daily life. For an infrastructure asset to be considered a national priority, both a high level of criticality and a high likelihood of something negative occurring must be demonstrated. Adopting a

risk-based approach for both prioritization of facilities through the likelihood of destruction and evaluation of national impacts can assist DHS in more effectively designating facilities as “critical.”

While infrastructure systems are interdependent, redundancy and resiliency also occur, which allow the larger systems to continue functioning during disruptions. Resiliency, or the ability of a facility to continue functioning, is the opposite of criticality. The ability of resilient systems to resume or continue functioning is the opposite of the failures and breakdowns in systems that DHS uses to frame the definitions of CI. This concept of resilience follows the *National Infrastructure Protection Plan*, which states, “resilient infrastructure systems are flexible and agile and should be able to bounce back after disruption.”²³¹ Within the resilient systems, disruptions that occur may cause beneficial changes. Policies centered on guarding a vast array of facilities from all types of risks potentially have the negative impact of preventing progress at the expense of protecting the status quo.

The 2013 *National Infrastructure Protection Plan* operates under the assumption that “both domestic and international critical infrastructure assets represent potential prime targets for adversaries. Given the deeply rooted nature of these goals and motivations, critical infrastructure likely will remain highly attractive targets for state and non-state actors and others with ill intent.”²³² Based on this research, IP efforts are framed under an inaccurate assumption of the terrorist threat to them. CI protection policies should not be the focus on large-scale attacks to facilities when they have not been the target of the largest domestic terrorist attacks and have rarely been the target of the 130,000 terrorist attacks across the world over the last 50 years. Terrorists have not previously targeted infrastructure and are unlikely to change their intentions in the future, which means that the way DHS views protecting infrastructure and preventing terrorism needs to be reformed.

²³¹ Department of Homeland Security, *Supplemental Tool: Executing a Critical Infrastructure Risk Management Approach*.

²³² Ibid.

D. OPPORTUNITY FOR FURTHER RESEARCH

Additional research into CI failures following the same methodology as the case studies within this thesis could determine if negligible losses, or even positive gains, occurred in a variety of circumstances. Looking at property values, tourism, tax revenue, hotel occupancy, and average rental prices of New Orleans, LA 10 years prior to and 10 years following Hurricane Katrina would likely show that the post-disaster city has made positive economic gains that positions it for a better future. Greensburg, KS was completely destroyed by an EF-5 tornado in 2007, but is now known to be a model green community because all the buildings have been built to the highest environment certification and are wind powered.²³³ It is unlikely that Greensburg would have become a national model of environmental sustainability without the tornado destroying all the town's existing infrastructure. In August 2007, the I-35 bridge over the Mississippi River in Minneapolis collapsed and traffic had to be rerouted until the replacement bridge opened in September 2008. The bridge would have been considered a critical component of the transportation infrastructure but the resiliency within the system allowed for traffic to be disrupted rather than a catastrophic failure of the entire system occurring.²³⁴ While sports stadiums and arenas are infrastructure considered critical to the local or regional economy, these facilities have been frequently demolished as facilities age or teams are sold then relocated. One example is the KeyArena in Seattle, WA, which housed the NBA Seattle SuperSonics from 1967–78, 1985–94, and 1995–2008, but continues to function in the interim periods without a team and still provides a venue for various forms of sports and entertainment today.²³⁵ Across the United States, large shopping malls were the hubs of commerce but many are vacant today.²³⁶ Many shopping malls

²³³ "Rebuilding Stronger, Better, Greener!" accessed August 31, 2015, <https://www.greensburgks.org/>.

²³⁴ "I-35W St. Anthony Falls Bridge," accessed August 31, 2015, <http://www.dot.state.mn.us/i35w/bridge/collapse.html>.

²³⁵ "KeyArena History," accessed August 31, 2015, <http://www.keyarena.com/arena-information/keyarena-history>.

²³⁶ Nelson D. Schwartz, "The Economics (and Nostalgia) of Dead Malls," *The New York Times*, January 4, 2015, http://www.nytimes.com/2015/01/04/business/the-economics-and-nostalgia-of-dead-malls.html?_r=0.

are considered CI by DHS but has the disappearance of the physical retail infrastructure resulted in economic losses to the surrounding areas?

Also, theoretical concepts should be explored based on the evidence presented within this thesis. If infrastructure systems have high levels of resilience and following disasters, areas are redeveloped in a more efficient and valuable manner, what would happen following a major cyber-attack that crippled the entire national power grid? While DHS and the Department of Energy work on strategies to harden the existing grid,²³⁷ would a catastrophic failure result in the creation of a decentralized and sustainable energy infrastructure? The seemingly worst-case scenario of losing the existing power grid could eventually result in an improved energy delivery system, which would position the country for a stronger future. The worst circumstances may spur the greatest opportunity for positive change, which could shift homeland security strategies to focus primarily on effective recovery rather than on protecting existing systems.

²³⁷ “Trustworthy Cyber Infrastructure for the Power Grid,” accessed August 31, 2015, <http://www.dhs.gov/science-and-technology/csd-tcipg>.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

- Abedine, Saad. "Yemen-based Al Qaeda Group Claims Responsibility for Parcel Bomb Plot." *CNN*, November 5, 2010. <http://www.cnn.com/2010/WORLD/meast/11/05/yemen.security.concern/>.
- Alliance for Downtown New York, Inc. *ADNY Annual Report 2014*. New York: Alliance for Downtown New York, Inc., 2014. http://www.downtownny.com/sites/default/files/Annual%20Report_2015_Final_Web2.pdf.
- . *Lower Manhattan Real Estate Market Overview 2014*. New York: Alliance for Downtown New York, Inc., 2014. <http://www.downtownny.com/sites/default/files/Q2%202014%20FINAL%20REPORT.pdf>.
- American Society for Quality. "Small Business Overview." 2015. <http://asq.org/learn-about-quality/small-business/overview/overview.html>.
- Appleseed. *Economic Impact of Redeveloping The World Trade Center Site: New York City, New York State, and the New York—New Jersey Area*. New York: Appleseed, 2003. <http://www.renewnyc.org/content/pdfs/Appleseed.pdf>.
- AxleGeeks. "Boeing 747–400 Freighter Commercial Cargo Jet." <http://planes.axlegeeks.com/1/279/Boeing-747-400-Freighter>.
- Bagli, Charles. "Guardian Insurance's Plan Adds to Downtown Rebirth." *The New York Times*, January 8, 1998. <http://www.nytimes.com/1998/01/09/nyregion/guardian-insurance-s-plan-adds-to-downtown-rebirth.html>.
- Bamber, David. "Bin Laden: Yes, I Did It." *The Telegraph*, November 11, 2001. <http://www.telegraph.co.uk/news/worldnews/asia/afghanistan/1362113/Bin-Laden-Yes-I-did-it.html>.
- Bay Area Water Supply & Conservation Agency. "Hetch Hetchy Water System." Accessed July 23, 2015. <http://bawsca.org/water-supply/hetch-hetchy-water-system/>.
- BBC News. "London Bombings Toll Rises to 37." July 7, 2005. <http://news.bbc.co.uk/2/hi/uk/4661059.stm>.
- . "Madrid Train Attacks: How the Attacks Happened." <http://news.bbc.co.uk/2/shared/spl/hi/guides/457000/457031/html/default.stm>.
- Belote, Howard D. "Warden and the Air Corps Tactical School—What Goes Around Comes Around." *AirPower Journal*, Fall 1999. <http://www.airpower.maxwell.af.mil/airchronicles/apj/apj99/fal99/belote.html>.

- Bin Laden, Osama. "Transcript: Translation of Bin Laden's Videotaped Message." *The Washington Post*, November 1, 2004. <http://www.washingtonpost.com/wp-dyn/articles/A16990-2004Nov1.html>.
- Bongar, Bruce Michael. *Psychology of Terrorism*. Oxford: Oxford University Press, 2007.
- Bram, Jason, James Orr, and Carol Raraport. "Measuring the Effects of the September 11 Attack on New York City." *FRBNY Economic Policy Review*, November 1, 2002. <http://www.newyorkfed.org/research/epr/02v08n2/0211rapa.pdf>.
- Building Owners and Managers Association International. "Building Class Definitions." Accessed July 23, 2015. <http://www.boma.org/research/Pages/building-class-definitions.aspx>.
- Bush, George W. "Statement by President George W. Bush in His Address to the Nation." September 11, 2001. <http://www.911memorial.org/sites/all/files/Statement>.
- Cabinet Office. *Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards*. United Kingdom: Cabinet Office, 2010. <https://www.gov.uk/government/publications/strategic-framework-and-policy-statement-on-improving-the-resilience-of-critical-infrastructure-to-disruption-from-natural-hazards>.
- Carr, Anthony B. "America's Conditional Advantage: Airpower, Countering Urgency, and the Theory of John Warden." Homeland Security Digital Library, June 1, 2009. <https://www.hsdl.org/?view&did=697900>.
- Center for Effective Government. "A Brief History of Administrative Government." 2015. <http://www.foreffectivegov.org/node/3461>.
- Centers for Disease Control and Prevention. *Disaster Response and Recovery Needs of Communities Affected by the Elk River Chemical Spill, West Virginia*. Atlanta, GA: Centers for Disease Control and Prevention, 2014. <http://www.dhhr.wv.gov/News/2014/Documents/WVCASPERReport.pdf>.
- Centre for Protection of National Infrastructure. "About: The National Infrastructure." Accessed July 23, 2015. <http://www.cpni.gov.uk/about/cni/>.
- City of Greensburg, KS. "Rebuilding Stronger, Better, Greener!" Accessed August 31, 2015. <https://www.greensburgks.org/>.
- City of New York Independent Budget Office. *Response to Request to Examine Critical Issues Underlying the Planned Rebuilding at the World Trade Center Site*. City of New York: Independent Budget Office, 2006. <http://www.ibo.nyc.ny.us/iboreports/stringerwtclet.pdf>.

- Clarion Project, The. "ISIS Releases Issue 6 of Dabiq Magazine." December 30, 2014. <http://www.clarionproject.org/news/islamic-state-isis-isil-propaganda-magazine-dabiq#>.
- CNN. "September 11th Fast Facts." March 27, 2015. <http://www.cnn.com/2013/07/27/us/september-11-anniversary-fast-facts/>.
- Coburn, Tom. *A Review of the Department of Homeland Security's Missions and Performance*. Washington, DC: United States Senate, 2015. <http://www.hsgac.senate.gov/download/?id=B92B8382>
- Coinnews Media Group LLC. "U.S. Inflation Calculator." Accessed July 23, 2015. <http://www.usinflationcalculator.com/>.
- Cole, Matthew. "Al Qaeda Promises U.S. Death by a 'Thousand Cuts'" *ABC News*, November 21, 2010. <http://abcnews.go.com/Blotter/al-qaeda-promises-us-death-thousand-cuts/story?id=12204726>.
- Davis Partners. "Key Office Properties." Accessed July 23, 2015. <http://davispartners.com/management/key-office-properties/>.
- Department of Defense. *The Department of Defense Critical Infrastructure Protection Plan Version 1.0*. Washington, DC: Department of Defense, 1998. <http://www.fas.org/irp/offdocs/pdd/DOD-CIP-Plan.htm>.
- Department of Homeland Security. "About: Infrastructure Information Collection Division." July 14, 2015. <http://www.dhs.gov/about-infrastructure-information-collection-division>.
- . *A Guide to Critical Infrastructure and Key Resources Protection at the State, Regional, Local, Tribal, and Territorial Level*. Washington, DC: Department of Homeland Security, 2008. http://www.dhs.gov/xlibrary/assets/nipp_srtl_t_guide.pdf.
- . *Commercial Facilities Risk Self-Assessment Tool*. Washington, DC: Department of Homeland Security, 2012. http://www.ahla.com/uploadedFiles/RSAT%20Fact%20Sheet_05172012.pdf.
- . "Countering Violent Extremism." July 20, 2015. <http://www.dhs.gov/topic/countering-violent-extremism>.
- . "Critical Infrastructure Sectors." June 12, 2014. <http://www.dhs.gov/critical-infrastructure-sectors>.

- . *Commercial Facilities Sector-Specific Plan an Annex to the National Infrastructure Protection Plan 2010*. Washington, DC: Department of Homeland Security, 2010. <http://www.dhs.gov/xlibrary/assets/nipp-ssp-commercial-facilities-2010.pdf>.
- . *FY 2013 Budget in Brief*. Washington, DC: Department of Homeland Security, 2013. <http://www.dhs.gov/xlibrary/assets/mgmt/dhs-budget-in-brief-fy2013.pdf>.
- . “Information Technology Sector.” June 12, 2014. <http://www.dhs.gov/information-technology-sector>.
- . *Interim National Infrastructure Protection Plan*. Washington, DC: Department of Homeland Security, 2005. <https://net.educause.edu/ir/library/pdf/csd3754.pdf>.
- . *National Infrastructure Protection Plan—Partnering to Enhance Protection and Resiliency*. Washington, DC: Department of Homeland Security, 2009. http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.
- . *National Infrastructure Protection Plan 2013—Partnering for Critical Infrastructure Security and Resilience*. Washington, DC: Department of Homeland Security, 2013. http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf.
- . “Protected Critical Infrastructure Information (PCII) Program.” June 18, 2014. <http://www.dhs.gov/protected-critical-infrastructure-information-pcii-program>.
- . “Protective Security Advisors.” June 23, 2015. <http://www.dhs.gov/protective-security-advisors>.
- . *Supplemental Tool: Executing a Critical Infrastructure Risk Management Approach*. Washington, DC: Department of Homeland Security, 2013. http://www.dhs.gov/sites/default/files/publications/NIPP%202013%20Supplement_Executing%20a%20CI%20Risk%20Mgmt%20Approach_508.pdf.
- . *Supplemental Tool: Incorporating Resilience into Critical Infrastructure Projects*. Washington, DC: Department of Homeland Security, 2013. http://www.dhs.gov/sites/default/files/publications/NIPP%202013%20Supplement_Incorporating%20Resilience%20into%20CI%20Projects_508.pdf.
- . *The 2014 Quadrennial Homeland Security Review*. Washington, DC: Department of Homeland Security, 2014. <http://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf>.
- . “Transportation Systems Sector.” March 25, 2013. <http://www.dhs.gov/transportation-systems-sector>.

- . “Trustworthy Cyber Infrastructure for the Power Grid.” Accessed August 31, 2015. <http://www.dhs.gov/science-and-technology/csd-tcipg>.
- . *Water Sector-Specific Plan An Annex to the National Infrastructure Protection Plan*. Washington, DC: Department of Homeland Security, 2010. <https://www.dhs.gov/xlibrary/assets/nipp-ssp-water-2010.pdf>.
- . “What is Critical Infrastructure?” August 26, 2015. <http://www.dhs.gov/what-critical-infrastructure>.
- . “What is Security and Resilience?” August 24, 2015. <http://www.dhs.gov/what-security-and-resilience>.
- Department of Numbers. “Las Vegas-Paradise Nevada Household Income.” Accessed July 23, 2015. <http://www.deptofnumbers.com/income/nevada/las-vegas/>.
- . “Las Vegas-Paradise Nevada Rent and Rental Statistics.” Accessed July 23, 2015. <http://www.deptofnumbers.com/rent/nevada/las-vegas/>.
- Department of the Interior. “Hoover Dam and Powerplant.” September 2013. <http://www.usbr.gov/lc/region/pao/brochures/hoover.html>.
- . “Hoover Dam—Frequent Asked Questions.” March 12, 2015. <http://www.usbr.gov/lc/hooverdam/faqs/damfaqs.html>.
- Environmental Protection Agency. “Vulnerability Self Assessment Tool (VSAT) 6.0.” September 4, 2014. <http://water.epa.gov/infrastructure/watersecurity/techtools/vsat.cfm>.
- Faber, Peter. “Competing Theories of Airpower: A Language for Analysis.” *AirPower Journal*, April 30, 1996. <http://www.airpower.maxwell.af.mil/%20airchronicles/presentation/faber.html>.
- Federal Emergency Management Agency. *National Protection Framework First Edition*. Washington, DC: Department of Homeland Security, 2014. http://www.fema.gov/media-library-data/1406717583765-996837bf788e20e977eb5079f4|174240/FINAL_National_Protection_Framework_20140729.pdf.
- . *World Trade Center 7 Building Performance Study*. Washington, DC: Department of Homeland Security, 2002. <http://www.fema.gov/media-library/assets/documents/3544>.
- Football Statistics Database Online. “Current NCAA Division 1 Football Teams.” 2010. <http://www.databasefootball.com/College/teams/teamlist.htm>.
- GbNYC Real Estate Group Commercial Real Estate. “One World Trade Center.” Accessed July 23, 2015. <http://www.greenbuildingsnyc.com/?page=121&cat=36>.

Gosselin, Peter. "Wall Street Hits the Wall As Financial World Spins, Leading Firms Depart the Nation's Economic Capital." *The Boston Globe*, June 28, 1996. <http://www.highbeam.com/doc/1P2-8373110.html>.

Government Accountability Office. *Critical Infrastructure Protection DHS Action Needed to Enhance Integration and Coordination of Vulnerability Assessment Efforts*. (GAO-14-507). Washington, DC: U.S. Government Accountability Office, 2014. <http://www.gao.gov/assets/670/665788.pdf>.

———. *Critical Infrastructure Protection—DHS List of Priority Assets Needs to be Validated and Reported to Congress*. (GAO-13-296). Washington, DC: U.S. Government Accountability Office, 2013. <http://www.gao.gov/assets/660/653300.pdf>.

———. *Critical Infrastructure Protection—DHS Efforts to Assess Chemical Security Risk and Gather Feedback on Facility Outreach Can Be Strengthened*. (GAO-13-353). Washington, DC: U.S. Government Accountability Office, 2013. <http://www.gao.gov/products/GAO-13-353>.

———. *Critical Infrastructure: Assessment of the Department of Homeland Security's Results of Its Critical Infrastructure Partnership Streamlining Efforts*. (GAO-14-100R). Washington, DC: U.S. Government Accountability Office, 2013. <http://www.gao.gov/assets/660/659074.pdf>.

———. *Federal Facility Cyber Security DHS and GSA Should Address Cyber Risk to Building and Access Control Systems*. (GAO-15-6). Washington, DC: U.S. Government Accountability Office, 2014. <http://www.gao.gov/assets/670/667512.pdf>.

———. *The Department of Homeland Security's Critical Infrastructure Protection Cost-Benefit Report*. (GAO-09-654R). Washington, DC: U.S. Government Accountability Office, 2009. <http://www.gao.gov/new.items/d09654r.pdf>.

Griggs, Brandon. "Fabled Las Vegas Casino Closes after 60 Years." *CNN*, May 5, 2015. <http://www.cnn.com/2015/05/05/travel/riviera-hotel-casino-vegas-closes-feat/>.

Harris County Office of Homeland Security and Emergency Management. *Lessons Learned Information Sharing, Infrastructure Systems: Developing a Critical Infrastructure and Key Resources (CIKR) Plan*. Houston, TX: Harris County Office of Homeland Security and Emergency Management, 2014. <http://www.readyharris.org/external/content/document/1829/2233754/1/20140825%20LLISI%20CKR.pdf>.

History.com. "Oklahoma City Bombing." A&E Television Networks. Accessed July 22, 2015. <http://www.history.com/topics/oklahoma-city-bombing>.

Hoffman, Bruce. *Inside Terrorism*. New York: Columbia University Press, 2006.

- Homeland Security Advisory Council. *Report of the Critical Infrastructure Task Force*. Washington, DC: Department of Homeland Security, 2006. http://www.dhs.gov/xlibrary/assets/HSAC_CITF_Report_v2.pdf.
- Homeland Security Council. *National Strategy for Homeland Security*. Washington, DC: The White House, 2007. http://www.dhs.gov/xlibrary/assets/nat_strat_homeland_security_2007.pdf.
- HVS Global Hospitality Services. *2012 Manhattan Hotel Market Overview*. Mineola, NY: HVS Global Hospitality Services, 2012. <http://www.hvs.com/Content/3268.pdf>.
- Institute of Transportation Engineers. "Ahead of the Storm: Engineering for Disaster." *ITE Journal*, 2013. <http://search.proquest.com/docview/1468925507?accountid=12702>.
- Jiang, Pu, and Yacov Y. Haimes. "Risk Management for Leontief-based Interdependent Systems." *Risk Analysis* 24, no. 5 (2004): 1215–1229. <http://dx.doi.org/10.1111/j.0272-4332.2004.00520.x>.
- Johnson, Jeh Charles. "Remarks By Secretary Jeh Charles Johnson On "The New Realities Of Homeland Security" As Part of the Landon Lecture Series on Public Issues—As Prepared for Delivery." Department of Homeland Security, May 27, 2015. <http://www.dhs.gov/news/2015/05/27/remarks-secretary-homeland-security-jeh-charles-johnson-%E2%80%9Cnew-realities-homeland>.
- Joseph. Anthony. "Critical Business Elements and Key Assets." *Security* 43, no. 8 (2006): 40–41. <http://search.proquest.com/docview/197794745?accountid=12702>.
- Kadri, Farid, Bibiga Birregah, and Eric Châtelet. "The Impact of Natural Disasters on Critical Infrastructures: A Domino Effect-based Study." *Journal of Homeland Security and Emergency Management* 11, no. 2 (2014): 217–241. <http://dx.doi.org/10.1515/jhsem-2012-0077>.
- KeyArena at Seattle Center. "KeyArena History." Accessed August 31, 2015. <http://www.keyarena.com/arena-information/keyarena-history>.
- Kristof, Nicholas. "A Guru's Journey—A Special Report; The Seer among the Blind: Japanese Sect Leader's Rise." *The New York Times*, March 25, 1995. <http://www.nytimes.com/1995/03/26/world/guru-s-journey-special-report-seer-among-blind-japanese-sect-leader-s-rise.html>.
- Las Vegas Convention and Visitors Authority. "Historical Las Vegas Visitor Statistics." February 1, 2015. <http://www.lvcva.com/stats-and-facts/>.
- Las Vegas Revealed. "Yet Another Las Vegas Casino History Timeline." Accessed July 23, 2015 http://www.lvrevealed.com/deathwatch/las_vegas_timeline.html.

- Lueck, Thomas. "Wall Street, No Longer Financial Epicenter, Struggles to Cling to Cachet." *The New York Times*, December 26, 1994. <http://www.nytimes.com/1994/12/27/nyregion/wall-street-no-longer-financial-epicenter-struggles-to-cling-to-cachet.html>.
- Markets and Markets. "Press Release: Critical Infrastructure Protection Market Worth \$ 114.30 Billion by 2019." 2015. <http://www.marketsandmarkets.com/PressReleases/critical-infrastructure-protection-cip.asp>.
- Mashayekhi, Rey. "Class A Rents in Midtown Rebound; Midtown South Sees 'Hitch'" *The Real Deal—New York Real Estate News*, May 1, 2015. <http://therealdeal.com/blog/2015/05/01/class-a-rents-in-midtown-rebound-while-midtown-south-sees-hitch/>.
- Mineta Transportation Institute. "Explosives and Incendiaries Used in Terrorist Attacks on Public Surface Transportation: A Preliminary Empirical Examination." March 1, 2010. <http://transweb.sjsu.edu/MTIportal/research/publications/documents/2875-IED-Support-Research.pdf>.
- Minnesota Department of Transportation. "I-35W St. Anthony Falls Bridge." Accessed August 31, 2015. <http://www.dot.state.mn.us/i35wbridge/collapse.html>.
- Moghaddam, Fathali M. *From the Terrorists' Point of View What They Experience and Why They Come to Destroy*. Westport, CT: Praeger Security International, 2006.
- Moteff, John. *Critical Infrastructure: The National Asset Database*. (CRS Report Order Code RL33648). Washington, DC: Congressional Research Service, 2007.
- Moteff, John, Claudia Copeland, and John Fischer, *Critical Infrastructures: What Makes an Infrastructure Critical?*. (CRS Report No. RL31556). Washington, DC: Congressional Research Service, 2003. <http://fas.org/irp/crs/RL31556.pdf>.
- National Conference of State Legislatures. "National Employment Monthly Update." July 2, 2015. <http://www.ncsl.org/research/labor-and-employment/national-employment-monthly-update.aspx>.
- National Highway Transportation Safety Administration. *Traffic Safety Facts 2013 Data*. Washington, DC: U.S. Department of Transportation, 2015. <http://www-nrd.nhtsa.dot.gov/Pubs/812181.pdf>.
- National Public Radio. "The Brothers' Examines Motivation Behind Boston Marathon Bombing." April 3, 2015. <http://www.npr.org/2015/04/03/397213144/-the-brothers-examines-motivation-behind-boston-marathon-bombing>.
- New World Encyclopedia. "World Trade Center." July 9, 2015. http://www.newworldencyclopedia.org/entry/World_Trade_Center.

- New York City Department of Finance. *Tentative Assessment Roll: Fiscal Year 2008*. New York: Department of Finance, 2007. http://www1.nyc.gov/assets/finance/downloads/pdf/07pdf/assessment_report_08.pdf.
- New York City—The Official Guide. “NYC Statistics.” Accessed July 23, 2015. <http://www.nycgo.com/articles/nyc-statistics-page>.
- New York State Education Department. “The World Trade Center—Facts and Figures.” Accessed July 22, 2015. <https://www.nysm.nysed.gov/wtc/about/facts.html>.
- Office of Inspector General. *Progress in Developing the National Asset Database*. (OIG-06-40). Washington, DC: Department of Homeland Security, 2006. http://www.oig.dhs.gov/assets/Mgmt/OIG_06-40_Jun06.pdf.
- Office of Tax Policy. *Annual Report: New York City Property Tax FY 2014*. City of New York: Department of Finance, 2014. http://www1.nyc.gov/assets/finance/downloads/pdf/reports/reports-property-tax/nyc_property_fy14fmvandav.pdf.
- . *Report on New York City Property Tax FY 2000*. City of New York: Department of Finance, 2000. <http://www1.nyc.gov/assets/finance/downloads/pdf/99pdf/rptsum00.pdf>.
- Office of the Inspector General. *Effectiveness of the Infrastructure Security Compliance Division’s Management Practices to Implement the Chemical Facility Anti-Terrorism Standards Program*. Washington, DC: Department of Homeland Security, 2013. https://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-55_Mar13.pdf.
- Parrish, Lee, and Mark Leary. “Secure Global Collaboration among Critical Infrastructures.” *Information Security Journal: A Global Perspective* 18, no. 2 (2009): 57–63. <http://search.proquest.com/docview/743437113?accountid=12702>.
- Public Broadcasting Service. “History of Biowarfare.” 2002. http://www.pbs.org/wgbh/nova/bioterror/hist_nf.html#cult.
- Rogers, Christopher D. F., Christopher J. Bouch, Stephen Williams. Austin R. G. Barber, Christopher J. Baker, John R. Bryson, David N. Chapman, Lee Chapman, Jon Coaffe, Ian Jefferson, and Andrew D. Quinn. “Resistance and Resilience-Paradigms for Critical Local Infrastructure.” *Proceedings of the Institution of Civil Engineers: Mechanical Engineering* 165, no. 2 (2012): 73–83. <http://search.proquest.com/docview/1223110482?accountid=12702>.
- Rothstein, Mervyn. “The Former Mobil Building, Largely Vacant in the 90’s, Gets a New Tenant. American Airlines.” *The New York Times*, October 29, 1996. <http://www.nytimes.com/1996/10/30/business/former-mobil-building-largely-vacant-90-s-gets-new-tenant-american-airlines.html>.

- Samuelson, William, and Richard Zeckhauser. "Status Quo Bias in Decision Making." *Journal of Risk and Uncertainty* 1 (1988): 7–59. <http://www.hks.harvard.edu/fs/rzeckhau/SQBDM.pdf>.
- Schwartz, David G. *Major Gaming Jurisdiction: Twelve-Year Comparison*. Las Vegas: Center for Gaming Research, University Libraries, University of Nevada Las Vegas, 2013. http://gaming.unlv.edu/reports/12_year_comp.pdf.
- Schwartz, Nelson D. "The Economics (and Nostalgia) of Dead Malls." *The New York Times*, January 4, 2015. http://www.nytimes.com/2015/01/04/business/the-economics-and-nostalgia-of-dead-malls.html?_r=0.
- Science Daily, CNRS (Délégation Paris Michel-Ange). "Pathological Gambling Caused by Excessive Optimism." April 29, 2013. <http://www.sciencedaily.com/releases/2013/04/130429102400.htm>.
- Sharot, Tali. "The Optimism Bias." *Science Direct*, 21, no. 23 (2011): R941–R945. <http://www.sciencedirect.com/science/article/pii/S0960982211011912>.
- Sharrock, David. "IRA Is Not So Ruthless and Always Gives Bomb Warnings." *The Telegraph*, September 19, 2001. <http://www.telegraph.co.uk/news/uknews/1340995/IRA-is-not-so-ruthless-and-always-gives-bomb-warnings.html>.
- Silverstein Properties. "Home: World Trade Center." Accessed July 23, 2015. <https://www.wtc.com/>.
- Stout, David. "Original Plan for 9/11 Attacks Involved 10 Planes, Panel Says." *The New York Times*, June 16, 2004. <http://www.nytimes.com/2004/06/16/politics/16CND-REPORT.html>.
- Thale, Richard H., and Cass R. Sunstein. *Nudge: Improving Decisions about Health, Wealth, and Happiness*. New Haven, CT: Yale University Press, 2008.
- U.S. Bureau of Labor Statistics. "Las Vegas-Paradise, NV Economy at a Glance." July 21, 2015. http://www.bls.gov/eag/eag.nv_lasvegas_msa.htm.
- U.S. Census Bureau. "Public Data from U.S. Census Bureau." Google.com. February 5, 2015, http://www.google.com/publicdata/explore?ds=kf7tgg1uo9ude_&met_y=population&idim=place:3240000:3260600:3231900&hl=en&dl=en#!ctype=l&strail=false&bcs=d&nselm=h&met_y=population&scale_y=lin&ind_y=false&rdim=country&idim=place:3240000:3260600:3231900&ifdim=country&tstart=1104642000000&tend=1372737600000&hl=en_US&dl=en&ind=false.
- U.S. Congressional Budget Office. *New Directions for the Nation's Public Works*. Washington, DC: U.S. Government Printing Office, 1988.

- . *Public Works Infrastructure: Policy Considerations for the 1980s*. Washington, DC: U.S. Government Printing Office, 1983.
- U.S. Green Building Council. “About: LEED Certification.” Accessed July 23, 2015. <http://www.usgbc.org/leed>.
- . “The Business Case for Green Building.” Accessed July 23, 2015. <http://www.usgbc.org/articles/business-case-green-building>.
- United Kingdom Cabinet Office. “A Summary of the 2014 Sector Resilience Plans.” August 1, 2014. <https://www.gov.uk/government/collections/sector-resilience-plans>.
- United Kingdom Government Digital Services. “Emergency Planning.” Accessed July 23, 2015. <https://www.gov.uk/government/policies/emergency-planning>.
- United States Congress. *Committee Reports 109th Congress (2005–2006) House Report 109-713—Part 1*. Washington, DC: The Library of Congress, Thomas, 2007. http://thomas.loc.gov/cgi-bin/cpquery/?&sid=cp109alJsu&r_n=hr713p1.109&d_bname=cp109&&sel=TOC_192496&.
- University of Maryland. “Global Terrorism Database, Search Results: 141966 Incidents.” Accessed July 22, 2015. <http://www.start.umd.edu/gtd/>.
- Urban Environmental Research, LLC. *Clark County: Critical Infrastructure & Key Assets Final*. Clark County, NV: Urban Environmental Research, LLC, 2008. http://www.clarkcountynv.gov/Depts/comprehensive_planning/nuclear_waste/Documents/Studies/CCCriticalInfrastructure0508.pdf.
- VegasClick.com. “Complete List of Las Vegas Casinos.” February 1, 2015. <http://vegasclick.com/vegas/casinos>.
- Warden, John A. “The Enemy As a System.” *AirPower Journal*, Spring 1995. http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/warden.htm.
- West Virginia Bureau for Public Health (WVBPH) and the Agency for Toxic Substances Disease Registry. *Elk River Chemical Spill Health Effects Findings of Emergency Department Record Review April 2014 Collaborative Investigation by the West Virginia Bureau for Public Health (WVBPH) and the Agency for Toxic Substances Disease Registry (ATSDR)*. West Virginia: Department of Health & Human Resources, 2014. <http://www.dhhr.wv.gov/News/chemical-spill/Documents/ElkRiverMedicalRecordSummary.pdf>.
- White House, The. *Homeland Security Presidential Directive 7*. Washington, DC: The White House, 2003. <http://www.dhs.gov/homeland-security-presidential-directive-7>.

- . *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection*. Washington, DC: The White House, 2003. <http://www.dhs.gov/homeland-security-presidential-directive-7>.
- . *Presidential Decision Directive/NSC-63*. Washington, DC: The White House, 1998. <http://www.fas.org/irp/offdocs/pdd/pdd-63.htm>.
- . *Presidential Policy Directive—Critical Infrastructure Security and Resilience Presidential Policy Directive/PPD-21—Critical Infrastructure Security and Resilience*. Washington, DC: The White House, 2013. <http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.
- Willis, Henry. *Terrorism Risk Modeling for Intelligence Analysis and Infrastructure Protection*. Santa Monica, CA: RAND Corporation, 2006. http://www.rand.org/content/dam/rand/pubs/technical_reports/2007/RAND_TR386.pdf.
- World Bank. “Current United States GDP.” 2015. <http://data.worldbank.org/indicator/NY.GDP.MKTP.CD>.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California